BB

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－216500
（P2003－216500A）
(43)公開日　平成15年７月31日(2003.7.31)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
G06F	12/14	320	G06F	12/14	320B　5B017
	17/60	142		17/60	142　5B035
		302			302E　5B058
		510			510　5J104
		512			512

審査請求　未請求　請求項の数７　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願2002－13650(P2002－13650)

(22)出願日　平成14年１月23日(2002.1.23)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　中出　真弓
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内

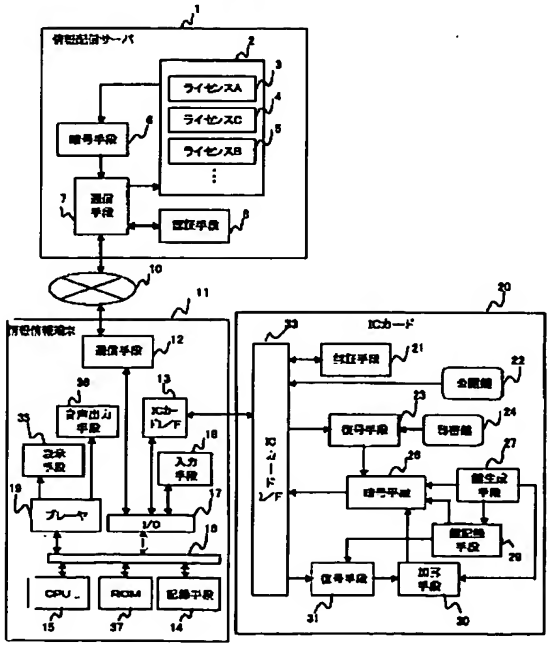
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　デジタル著作権管理システム

(57)【要約】
【課題】従来のデジタル著作権保護システムでは、購入ライセンス数が増えると、セキュアなカードで管理するデジタルライセンスデータ数が増え、多くの容量が必要になる。
【解決手段】本発明においては、複数のライセンスデータを暗号化する為の複数の鍵データをまとめて１個の鍵束鍵データで暗号化する。ＩＣカードでは、前記鍵束データだけを管理し、ライセンスを暗号化したデータおよび暗号化するのに用いた鍵データをまとめて暗号化したデータは情報処理装置に格納する。以上の手段により、ＩＣカードには１個の鍵束データを記録するだけで複数のライセンスを管理することができる。また、暗号化されたライセンスおよび鍵束は、暗合する時に使用したＩＣカードを合わせて使用するときのみ有効である為、他者のライセンスの不正利用はできず、ＩＣカード保持者のみ容易に複写，再生が可能である。

【図１】



【特許請求の範囲】
【請求項１】秘密鍵および該秘密鍵に対応した公開鍵が記録されたＩＣカードと、該ＩＣカードとの接続手段およびデータ通信手段とを備えた情報処理装置と、複数個のライセンスデータが格納され前記情報処理装置に前記通信手段を介してライセンスデータを配信するライセンス配信装置とで構成され、
前記ライセンス配信装置にはライセンスデータを前記ＩＣカードの公開鍵で暗号化して第１の暗号化ライセンスデータとする第１の暗号化手段と、前記第１の暗号化ライセンスデータを前記情報処理装置に配信するライセンス配信手段を設け、前記情報処理端末は、前記ライセンス配信装置より配信された第１の暗号化ライセンスデータを前記ＩＣカードに渡し、前記ＩＣカードには、前記ライセンス配信装置から配信された第１の暗号化ライセンスデータを前記秘密鍵で復号化してライセンスデータとする復号化手段と、前記ライセンスデータ毎に鍵データを生成する鍵データ生成手段と、前記ライセンスデータを前記鍵データで暗号化して第２の暗号化ライセンスデータを生成する第２の暗号化手段と、前記ライセンスデータ毎の前記鍵データをまとめて１個の鍵束データとする鍵束データ生成手段とを設け、
前記鍵データ生成手段で前記作成した鍵束データ毎に鍵束鍵データを生成し、該鍵束鍵データを鍵データとして前記第２の暗号化手段で、前記鍵束データを暗号化して暗号化鍵束データを生成し、前記鍵束鍵データをＩＣカードに記録することを特徴としたデジタル著作権管理システム。
【請求項２】請求項１におけるデジタル著作権管理システムであって、
前記ＩＣカードの第２の暗号化手段で生成された、第２の暗号化ライセンスデータおよび前記暗号化鍵束データを前記情報処理装置に記録することを特徴としたデジタル著作権管理システム。
【請求項３】請求項１および請求項２のデジタル著作権管理システムであって、ＩＣカードに前記暗号化鍵束データを前記鍵束鍵データで複合化する第２の複合化手段を設け、
前記ＩＣカードは前記情報処理装置から前記第２の暗号化ライセンスデータを受け取る毎に、前記鍵束鍵データで前記鍵束データ前記鍵生成手段で新たな鍵データおよび新たな鍵束鍵データを生成し、該新たに生成された鍵データを前記鍵束データ生成手段で鍵束データに追加して新たな鍵束データとし、該新たな鍵束データを前記新たな鍵束鍵データを用いて前記第２の暗号化手段で暗号化して新たな暗号化鍵束データを生成し、前記鍵束鍵データをＩＣカードに記録するとともに、古い鍵束鍵データである前記鍵束鍵データを記録から削除することを特徴としたデジタル著作権管理システム。
【請求項４】請求項１および請求項２、請求項３のデジタル著作権管理システムであって、前記情報処理装置からのライセンスデータ削除要求あるいは移動要求に応じて、前記ＩＣカードは前記鍵束鍵データを用いて前記暗号化鍵束データを前記複合化手段で複合化して鍵束データとし、前記削除要求あるいは移動要求があったライセンスデータに対応した鍵データを前記鍵データから削除して新たな鍵束データを作成し、前記鍵生成手段で新たな鍵束鍵データを生成し、該新たな鍵束鍵データを用いて前記新たな鍵束データを前記第２の暗号化手段で暗号化して新たな暗号化鍵束データとして前記情報処理装置に記録し、前記新たな鍵束鍵データは前記ＩＣカードに記録するとともに前記鍵束鍵データを消去することを特徴としたデジタル著作権管理システム。
【請求項５】請求項１および請求項２、請求項３、請求項４のデジタル著作権管理システムであって、
前記ＩＣカードに公開鍵でデータを暗号化する第３の暗号化手段を設け、
第２の情報処理装置にライセンスデータを移動するときには、前記第２の情報処理装置に接続する第２のＩＣカードの公開鍵を用いて移動する前記ライセンスデータを前記第３の暗号化手段で暗合することを特徴としたデジタル著作権管理システム。
【請求項６】秘密鍵と、該秘密鍵に対応した公開鍵と、該公開鍵で暗号化された暗号化データを前記秘密鍵で復号化して平分データとする復号化手段と、前記平分データ毎に鍵データを生成する鍵データ生成手段と、前記ライセンスデータを前記鍵データで暗号化して第２の暗号化データを生成する暗号化手段と、前記平分データ毎の前記鍵データをまとめて１個の鍵束データとする鍵束データ生成手段とを設け、前記鍵データ生成手段で前記作成した鍵束データ毎に鍵束鍵データを生成し、該鍵束鍵データを鍵データとして前記第２の暗号化手段で、前記鍵束データを暗号化して暗号化鍵束データを生成し、前記鍵束鍵データをＩＣカードに記録することを特徴としたＩＣカード。
【請求項７】ＩＣカードに秘密鍵と、該秘密鍵に対応した公開鍵と、該公開鍵で暗号化された暗号化ライセンスデータを前記秘密鍵で復号化してライセンスデータとする復号化手段と、前記ライセンスデータ毎に鍵データを生成する鍵データ生成手段と、前記ライセンスデータを前記鍵データで暗号化して第２の暗号化データを生成する暗号化手段と、前記ライセンスデータ毎の前記鍵データをまとめて１個の鍵束データとする鍵束データ生成手段とを設け、前記鍵データ生成手段で前記作成した鍵束データ毎に鍵束鍵データを生成し、該鍵束鍵データを鍵データとして前記第２の暗号化手段で、前記鍵束データを暗号化して暗号化鍵束データを生成し、前記鍵束鍵データをＩＣカードに記録することを特徴とし、前記ＩＣカードとの接続手段を有する情報処理装置には前記第２の暗号化ライセンスデータおよび前記暗号化鍵束データ

を記録することを特徴としたデジタル著作権管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル化された動画や音声等のコンテンツの著作権を保護するデジタル著作権管理システムに関し、特に、ＩＣカードを用いて著作権を保護するデジタル著作権管理システムに関する。

【０００２】

【従来の技術】従来のデジタル化された動画や音声等のコンテンツの著作権を保護するデジタル著作権を保護する為のシステムとしては、ケイタイdeミュージック・コンソーシアムが規格化したケイタイdeミュージックによるコンテンツ配信サービスがある。

【０００３】上記、ケイタイdeミュージックでは、無料の暗号化コンテンツが携帯電話網を介してコンテンツサーバから配信される。暗号化コンテンツを復号化する鍵であるライセンスは、ユーザがライセンスの権利を購入すると、携帯電話網を介して暗号化されたライセンスがライセンスサーバから配信される。配信された暗号化ライセンスは、携帯電話を介してセキュアなメモリーカードに入力され、復号化されて格納される。コンテンツをプレーヤで再生する場合は、前記メモリーカードから暗号化コンテンツ及びライセンスを呼出し、暗号化コンテンツをライセンスで復号化して再生する。

【０００４】

【発明が解決しようとする課題】上記従来の著作権保護システムでは、ライセンスは全てメモリーカードに格納する為、メモリーカードの容量により、格納できるライセンスの数が限られる。特に、容量が比較的小さいＩＣカード等では、多くのライセンスを購入するには、複数枚のカードをもつ必要がある。また、上記発明では、ライセンスを他人に譲渡する場合について考えられておらず、ユーザにとってあまり使い勝手のいいシステムではなかった。

【０００５】本発明の目的は、携帯が容易な小さな記録容量のＩＣカード等でＩＣカードの記録容量より多くのライセンスを管理することができ、また、暗号化ライセンスを安全に管理でき、さらに、ＩＣカード所有者は自分が所有する複数の機器に暗号化ライセンスをコピーすることでＩＣカードを持ち歩くだけで、どこでもコンテンツの再生ができるデジタル著作権管理システムを提供することにある。

【０００６】

【課題を解決するための手段】上記課題を解決する為に、本発明のデジタル著作権管理システムの１つの特徴として、ライセンス購入時にはサーバから受け取った暗号化ライセンスをＩＣカード上で秘密鍵を用いて復号化したのち、乱数発生手段により新たなライセンス鍵を生成し、そのライセンス鍵で復号化したライセンスを再び暗号化し、その再び暗号化したライセンスを情報処理端末に蓄積する。複数個のライセンスを保有する場合は、ＩＣカードでは、ライセンス鍵束鍵を生成し、前記複数個のライセンス鍵をまとめて暗号化し、そのまとめて暗号化したライセンス鍵を情報処理端末に蓄積する。ＩＣカードにはライセンス鍵束鍵を蓄積する。

【０００７】以上のようなライセンス蓄積方法により、蓄積容量の少ないＩＣカードでも多くのライセンスを管理できる。

【０００８】

【発明の実施の形態】以下、本発明の実施例について、図面を用いて説明する。

【０００９】図１は本発明の第一の実施例であるデジタル著作権管理システムの機能ブロック図である。１は情報配信サーバ、１０はネットワーク、１１は情報処理端末、２０はＩＣカードであり、情報配信サーバ１および情報処理端末１１はネットワーク７で接続され、ＩＣカード２０は情報端末１１に接続している。以下、それぞれの構成について説明する。

【００１０】情報配信サーバ１には、少なくとも、記録手段２、暗号化手段６、認証手段８および通信手段７がある。情報配信サーバ１は、通信手段７で受信した要求に従い、認証手段８でのＩＣカードの認証、暗号化手段６による記録手段２に格納されているライセンスの暗号化、および通信手段７を介した暗号化したライセンスの送信をおこなう。

【００１１】情報端末１１には、少なくとも、ＣＰＵ１５およびＣＰＵ１５とバス１６で接続するＲＯＭ３７、記録手段１４、Ｉ／Ｏ１７、再生手段１９と、Ｉ／Ｏ１７で制御される入力手段１８、ＩＣカードＩ/Ｆ１３、通信手段１２、表示装置３５、音声出力手段３６で構成される。記録手段１２は、例えば、書き換え可能なＲＡＭや、ハードディスク、フラッシュＲＯＭであり、入力手段は、操作ボタンあるいはタッチパネル等である。前記ＩＣカードＩ／Ｆ１３はＩＣカード２０と接続し、通信手段１２は情報配信サーバ１とネットワーク１０で接続する。

【００１２】ＩＣカード２０には、少なくとも、情報端末１１と接続する為の入出力Ｉ／Ｆ２３、情報配信サーバ１を認証する為の認証手段２１、情報配信サーバ１の暗号化手段６がライセンスを暗号化する為の使う公開鍵２２、および公開鍵２２に対応した秘密鍵２４、秘密鍵２４を使って暗号化ライセンスを復号化する為の復号化手段２３、複数の鍵データを生成する鍵生成手段２７、鍵生成手段２７で生成した鍵データでデータの暗号化処理を行う暗号化手段２６、鍵生成手段２７で生成した鍵データの幾つかをまとめて鍵束データを作成する加算手段３０、前記鍵束データを暗号化する際の鍵である鍵束鍵データを記録する鍵記録手段２９、暗号化された鍵束データを情報端末１１の記録手段１４より呼び出す、鍵

束データ呼出し手段４０、鍵記録手段に記録されている鍵束鍵データで入力データを復号化する復号化手段３１がある。

【００１３】図１の著作権管理システムにおけるライセンスを要求してから、ＩＣカードがライセンスを入手するまでの手順について、図２を用いて説明する。

【００１４】図２は本発明の第1の実施例におけるライセンス入手処理の為のフローチャートである。１０１、１０２および１０３はそれぞれ図1の情報配信サーバ１、情報端末５およびＩＣカード２０における処理を示している。

【００１５】ライセンスを入手する場合は、図１の情報端末１の入力手段１８を用いてユーザがライセンス要求の意思表示をすると、情報端末１は情報配信サーバ１にライセンス要求送信を行う。ここで、ライセンス要求受信１１１を行った情報配信サーバ1は、ＩＣカード２０の認証処理１１２を行い、ＩＣカード２０でも同様に情報配信サーバ1の認証処理１３０を行う。認証処理１１２および認証処理１３０の具体的な処理例は後で説明する。

【００１６】認証処理１１２が終了する情報配信サーバ１は情報処理端末５にコンテンツＩＤ要求送信１１３を行う。ここで、図２では、情報配信サーバ1が要求するデータとしてコンテンツＩＤとしているが、コンテンツ名等、コンテンツが特定できるデータならばなんでもよい。コンテンツＩＤ要求受信１１４を行った情報処理端末5は、既に要求するコンテンツが決まっていればコンテンツＩＤ送信１１５を行う。ここで、情報配信サーバ１はコンテンツＩＤ要求送信１１３の代わりに、情報配信サーバがライセンスを管理しているコンテンツリストを情報処理端末に送信し、コンテンツリストが送られてきた時点でユーザがコンテンツリストからコンテンツを選択する形式としてもよい。この場合、情報処理端末５では表示装置３５にコンテンツリストを表示し、ユーザにコンテンツを指定するように促し、ユーザが入力手段１８を用いて入力したデータからコンテンツを特定し、情報配信サーバ１にコンテンツＩＤ送信１１５を行う。コンテンツＩＤ受信１１６を行った情報配信サーバ１は、コンテンツＩＤからライセンス検索１１７を行い、ライセンスデータを取り出し、ＩＣカード９の公開鍵２２でライセンス暗号化処理を行う。暗号化ライセンスは情報処理端末５で受信した後、ＩＣカード２０に送信する。

【００１７】次に、情報処理端末５およびＩＣカード９での暗号化ライセンス記録手順について、図３、図４を用いて説明する。

【００１８】図３は、本発明の第１の実施例における初めて入手するライセンス記録処理のフローチャートである。

【００１９】図２と同じものには同じ番号を付してある。情報処理端末１１は暗号化ライセンス受信１２９を行った後、情報処理端末１１の記録手段１４に記録せずにＩＣカード２０に暗号化ライセンス送信２０３を行う。ＩＣカードは暗号化ライセンス受信２０４を行った後、公開鍵１３０に対応した秘密鍵２０６でライセンス複合化処理２０５を行い、暗号化ライセンスの複合化を行う。次に、ＩＣカード２０では、鍵生成手段２７によりライセンス鍵生成２０７を行い、ライセンス暗号化処理２０９で、ライセンス毎のライセンス鍵２０８を生成する。このライセンス鍵２０８を用いて、暗号手段２６で前期複合化したライセンスの再暗号化を行う。次に、暗号化ライセンス送信２１０を行い、情報処理端末１１に再暗号化したライセンスを送信する。情報処理端末１１では、暗号化ライセンス受信２１１を行ったのち、暗号化ライセンス記録２１２を行い、ライセンス毎に異なるライセンス鍵で暗号化した前記再暗号化ライセンスを情報処理端末１１の記録手段に記録する。

【００２０】ＩＣカード２０では、暗号化ライセンス送信２１０を行った後、複数のライセンス鍵２０８を加算手段３０でまとめて、暗号手段２６で暗号化した暗号化鍵束を情報処理端末１１に要求する、暗号化鍵束要求送信２１３を行う。携帯情報端末２０１は暗号化鍵束要求を受信２１４した後、暗号化鍵束はまだないので、暗号化鍵束部分がからの暗号化鍵束送信２１５を行う。ＩＣカード２０は、からの暗号化鍵束受信２１６を行うと、鍵束用の鍵を生成する鍵束生成２２０を行う。この時生成した鍵束鍵ａ２２１はＩＣカードの鍵記録手段２９によりＩＣカード２０内に記録される。次に、ＩＣカード２０は鍵束鍵ａ２２１を用いて、ライセンス鍵２０８を暗号化する鍵束暗号化処理２２２を行う。ここで、暗号化されたライセンス鍵は暗号化鍵束として情報処理端末１１に送信する暗号化鍵束送信処理２２３を行う。情報処理端末１１では、暗号化鍵束受信２２４で、ＩＣカード２０から暗号化鍵束を受け取った後、暗号化鍵束を記録手段１４に記録する暗号化鍵束記録２２５を行う。

【００２１】以上、初めてライセンスを入手する際の、ライセンス記録処理に関して説明を行った。なお、上記ＩＣカード２０の暗号化鍵束要求送信２１３は、ＩＣカード２０側で、ライセンス入手がはじめて、あるいは情報処理端末５に記録されているライセンスがないことを、例えば、ＩＣカード２０に鍵束鍵が記録されていない等により、確認することにより、暗号化鍵束受信２１６とともに省略することができる。

【００２２】次に、情報処理端末５にすでにライセンスが記録されている場合について、図４を用いて説明する。図４は、本発明の第１の実施例におけるライセンス記録処理のフローチャートである。図３と同じ処理には同じ番号を付しており、情報処理端末５の暗号化鍵束送信２１４までは図３と同様なので説明は省略する。なお、本発明では、ライセンス鍵はライセンス毎に生成す

るので、図3のライセンス鍵２０８と図４のライセンス鍵２３０は異なるデータの鍵である。

【００２３】情報処理端末５は、すでに記録されている暗号化鍵束２２８をＩＣカードに送信する暗号化鍵束送信２２８を行う。ＩＣカード２０は暗号化鍵束受信２１６により受け取った暗号化鍵束２２８を鍵束鍵２２１を用いて復号化する処理である暗号化鍵束復号化２１７を復号手段３１で行い、復号化した鍵束にライセンス鍵２３０を加算手段３０で加算する処理であるライセンス鍵追加処理２１９を行う。さらに、ＩＣカード２０では新たに鍵束鍵を生成する鍵生成手段２７により鍵束鍵生成処理２２２を行い、鍵束鍵２３１を生成する。なお、本発明では、鍵束鍵は鍵束を新しくする毎に新たな鍵を生成し、鍵束鍵２２１と鍵束鍵２３１は異なるデータで構成される。

【００２４】ＩＣカード２０では、暗号化手段２６で新たに作成した鍵束鍵２３１で新たに作成した鍵束を暗号化する鍵束暗号化処理２２２を行い、情報処理端末５に送信する暗号化鍵束送信２２４を行う。情報処理端末５では、新たな暗号化鍵束を受け取る暗号化鍵束受信２２４を行い、暗号化鍵束２２８に替えて新たな暗号化鍵束２３２を記録する暗号化鍵束記録を行う。ＩＣカード２０では、暗号化鍵束送信２２３を行った後、古い鍵束鍵２２１を破棄し、新しい鍵束鍵２３１を鍵束鍵２２１として記録する。

【００２５】以上、本発明によるライセンス記録方法について説明した。本発明の記録方法では、ライセンスは異なる鍵で暗号化されている為、一つに鍵が破られてもすべてのライセンスを取り出すことができない。また、ＩＣカードに記録されているのは最低１個の鍵束鍵であるので、容量の少ないＩＣカードにおいても多くのライセンスを管理するシステムを構成することができる。

【００２６】次に、コンテンツの再生について説明する。図５は本発明の第一の実施例における、コンテンツ再生処理フロー例を示す。

【００２７】情報処理端末５はユーザからのコンテンツ再生命令により、ＩＣカード２０にコンテンツＩＤ３０５と共に、コンテンツを再生する為の処理を開始するコンテンツ再生要求送信３０３を行う。なお、コンテンツＩＤ３０５は後から送信しても良い。ＩＣカード２０はコンテンツ再生要求３０４を受信すると、コンテンツ再生に必要なライセンスを取り出す為に、暗号化鍵束２２８を得る為に、情報処理端末５に暗号化鍵束要求送信２１３を行う。情報処理端末５は暗号化鍵束要求受信２１４を行うと、暗号化鍵束２２８をＩＣカード２０に送信する暗号化鍵束送信２１５を行う。なお、前記暗号化鍵束要求送信２１３は、コンテンツ再生処理準備ができたことの応答等のメッセージでもかまわない。ＩＣカード２０は暗号化鍵束受信２１６を行うと、暗号化鍵束２２８を鍵記録手段２９に記録してあった鍵束鍵２２１を用いた復号化処理である暗号化鍵復号化２１７を行い、復号化された鍵束から、既に入手しているコンテンツＩＤ３０５に対応したライセンス３２０を取り出す該当ライセンス抽出３１０を行う。次ぎに、ＩＣカード２０はライセンスの送信を行う為の準備を行う。まず、ライセンスを暗号化する為、プレーヤの公開鍵要求送信３１１を行う。プレーヤ公開鍵要求受信３１２を行った情報処理端末１１はプレーヤ公開鍵３１４をＩＣカード２０に送信するプレーヤ公開鍵送信３１３を行う。プレーヤ公開鍵受信３１５を行ったＩＣカード２０は、プレーヤ公開鍵３１４で先に復号化したライセンス３２０を暗号化するライセンス暗号化処理３１６を行い、暗号化ライセンス３２１を情報処理端末に送信する暗号化ライセンス送信を行う。暗号化ライセンス受信３１８を行った情報処理端末１１は暗号化ライセンスをプレーヤ公開鍵３１４に対応したプレーヤ秘密鍵３４０で復号化するライセンス復号化処理３１９を行い、ライセンス３２０を取出し、暗号化コンテンツ３３０をライセンス３２０で復号化するコンテンツ復号化処理３２２を行い、コンテンツ３３１を取出し、そのコンテンツ３３１を音声あるいは映像にするコンテンツ再生３２３を行う。

【００２８】以上説明したように、本発明では、ライセンスをＩＣカード内ではなく携帯情報端末１１に格納する為、ＩＣカードにはライセンスをまとめた鍵のみを格納する方式である為、ＩＣカードの容量に無関係にライセンスを管理できる。また、ライセンスはライセンス毎異なる鍵で暗号化されているため、一つの鍵がわかっても、全ての鍵を解読することはできない。さらに、暗号化するたびに鍵が変わるのでより、安全なシステムにできる。

【００２９】次に、ライセンスを削除する場合について、図６を用いて説明する。

【００３０】図６は、本発明の第１の実施例のデジタル著作権管理システムのライセンス削除処理フロー例を示す。４０１は情報処理端末の処理、４０２はＩＣカード２０内の処理を示す。また、図４と同様の処理には、同じ番号を付しており説明は省略する。

【００３１】ユーザがコンテンツ削除あるいはコンテンツ移動命令を入力手段１８より入力すると、情報処理端末１１は削除するコンテンツＩＤ４０５とともに、コンテンツ削除要求送信４０３を行う。コンテンツ削除要求受信を行ったＩＣカード２０は、情報処理端末１１に暗号化鍵束要求送信２１３を送信する。以下、図４と同様に、情報処理端末１１で、暗号化鍵束要求受信２１４および暗号化鍵束送信２１５、ＩＣカード２０で暗号化鍵束受信２１６、暗号化鍵束復号化２１７を行う。次ぎに、ＩＣカード２０では復号化された、鍵束である暗号化ライセンスの束から、既に入手すみであるコンテンツＩＤ４０５に対応するライセンスを取り出し、残りのライセンスを新たな鍵束としてたばねる為の新たな鍵束鍵

を生成する鍵束生成４１６をおこない、新鍵束鍵で４１７で新たな鍵束を暗号化する鍵束暗号化処理４１８を行い、新暗号化鍵束４１９を生成し、暗号化鍵束送信４２１を行う。ＩＣカード２０では、暗号化鍵束送信４２１を行った後、新鍵束鍵４１７を鍵束鍵２２１と置換える鍵束鍵入替４２６を行い、さらに、取り出したライセンスの削除を行う。情報処理端末１１は、暗号化鍵束受信４２２を行った後、新暗号化鍵束４２３を暗号化鍵束２２８と置換える暗号化鍵束入替４２４を行う。

【００３２】以上説明したライセンス削除の方式により、削除するライセンスはＩＣカード内で処理、削除されるため、ユーザがライセンスを不正に利用することはできない。また、鍵束鍵が新たに作成され、新しい鍵束のみ有効となるため、古い鍵束をコピーしていたとしても、使用することができないので、ライセンスの削除を徹底できる。また、新たな鍵束をコピーすることで、有効なＩＣカードを持っていれば、他の情報処理端末等でライセンスを有効にすることができ、ユーザにとって使い勝手がよい。

【００３３】次に、ライセンスを他人に譲渡する場合について図７、図８を用いて説明する。

【００３４】図７は、本発明の第一の実施例におけるライセンスを譲渡する場合の構成例である。

【００３５】情報処理端末１１、ＩＣカード２０は既に図１で説明したものであり、情報処理端末５０は情報処理端末１１と同様の機能を有し、ＩＣカード５１はＩＣカード２０と同様の機能を有す。情報処理端末１１と情報処理端末５０は、各々の通信手段で、無線あるいは有線で接続し、データの交換を行う。次ぎに図８を用いて、ライセンスの譲渡処理について説明する。

【００３６】図８は、本発明の著作権管理システムにおけるライセンスを他人に譲渡する場合の処理フローを示す。ライセンスを渡す側の情報処理端末１１の処理を５０１、ＩＣカード２０の処理を５０２、ライセンスを受け取る側の情報処理端末５０およびのＩＣカード５１処理を５０３に示す。

【００３７】ユーザからの入力により、情報処理端末１１がライセンス移動要求５１０を行い、ＩＣカード２０がライセンス要求受信５１１が行われると、情報処理端末１１とＩＣカード２０で、図６で説明したライセンス削除処理５１２が行われる。但し、ライセンス削除４２７の処理はすぐには行われない。情報処理端末１１は情報処理端末５０に公開鍵要求送信５１４を行う。公開鍵要求受信５１５を行った情報処理端末５０はＩＣカード５１に記録されている公開鍵５１７を送る公開鍵送信５１６を行う。公開を受信した情報処理端末１１は、公開鍵をそのままＩＣカード２０に送信する。公開鍵受信５１８を行ったＩＣカード２０は、受信した公開鍵５１７で、既に取り出し済のライセンス５１３を暗号化するライセンス暗号化５２１を行い、暗号化ライセンス送信５２１を行う。また、ＩＣガード２０は暗号化ライセンス送信５２１を行った後、送信したライセンス削除５２を行う。情報処理端末１１は、ＩＣカード２０から受け取った暗号化ライセンス５２０をそのまま情報処理端末５０に送信する。暗号化ライセンス受信５２２を行った情報処理端末５０は、暗号化ライセンス５２０をＩＣカード５１に送り、情報処理端末５０およびＩＣカード５１で暗号化ライセンス記録処理５２３を行う。ここで、暗号化ライセンス記録処理５２３は図２あるいは図３で説明した処理と同様である為、説明は省略する。

【００３８】以上説明したように、本発明の著作権管理システムでは、ライセンスをＩＣカード内で、譲渡するＩＣカードの公開鍵で暗号化し、送信する為、譲渡先のＩＣカード以外にライセンスの内容がわからず、ライセンスを安全に送信することができる。また、ライセンスを削除で説明した時と同様、ライセンスを移動するたびに鍵束鍵が変わるので、不正なライセンス使用が容易にできない。

【００３９】

【発明の効果】以上説明したように、本発明のデジタル著作権管理システムにより、携帯が容易な小さな記録容量のＩＣカード等でＩＣカードの記録容量より多くのライセンスを管理することが出来る。また、携帯情報端末に記録された暗号化データは、鍵を作成したＩＣカードでしか複合化できないため、暗号化ライセンスを安全に管理できる。さらに、ＩＣカード所有者は自分が所有する複数の機器に暗号化ライセンスをコピーすることでＩＣカードを持ち歩くだけで、どこでもコンテンツの再生が可能である。

【図面の簡単な説明】

【図１】本発明の第一の実施例であるデジタル著作権管理システムの機能ブロック図である。

【図２】本発明の第1の実施例におけるライセンス入手処理の為のフローチャートである。

【図３】本発明の第１の実施例における初めて入手するライセンス記録処理のフローチャートである。

【図４】本発明の第１の実施例におけるライセンス記録処理のフローチャートである。

【図５】本発明の第１の実施例における、コンテンツ再生処理フロー例を示す。

【図６】本発明の第１の実施例におけるのライセンス削除処理フロー例を示す

【図７】本発明の第１の実施例におけるライセンスを譲渡する場合の構成例である。

【図８】本発明の第１の実施例におけるライセンスを譲渡する場合の構成例である。

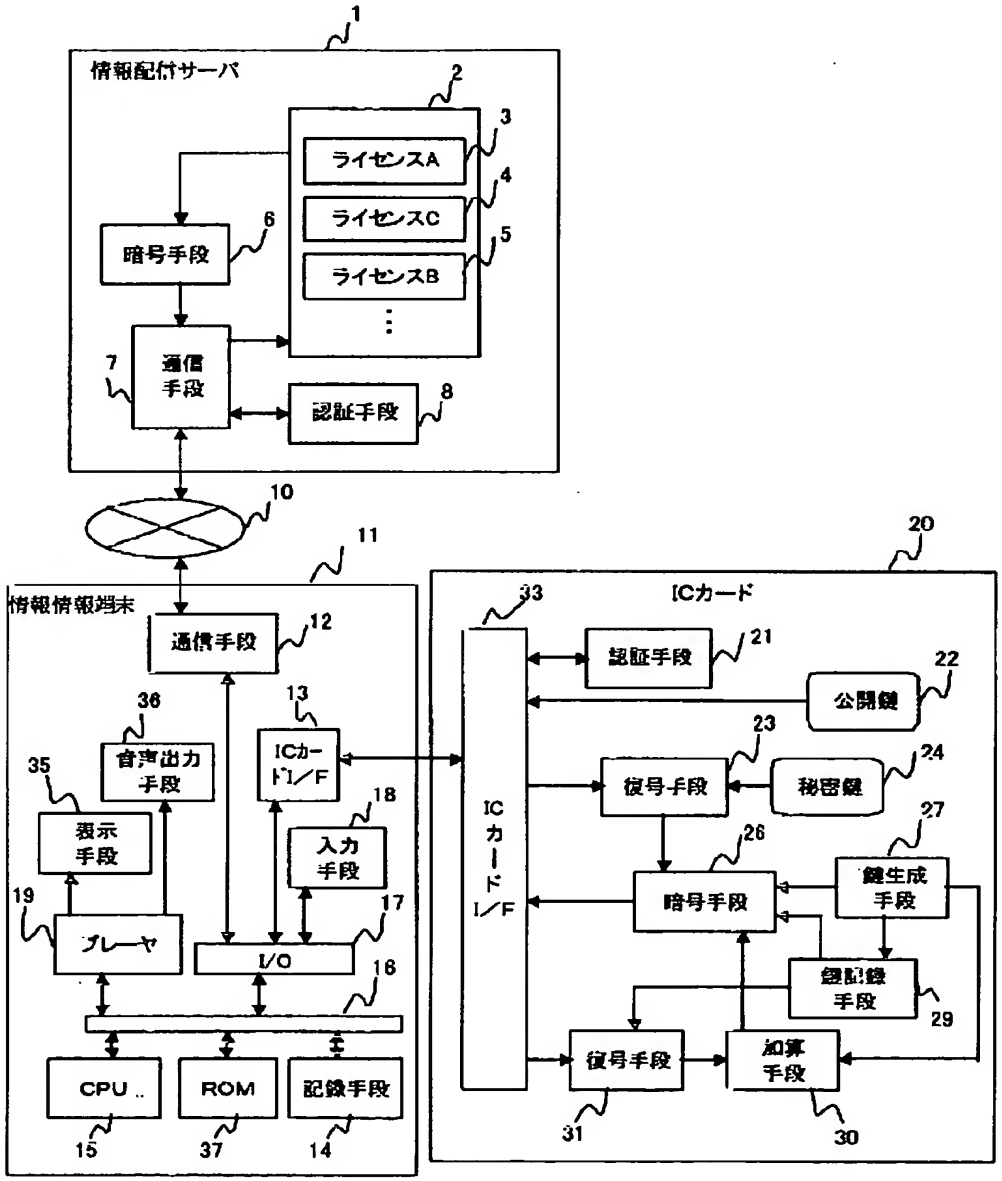
【符号の説明】

１…情報配信サーバ、１１…情報処理端末、６…暗号手段、７…通信手段、１０…公衆回線、１３…ＩＣカードＩ／Ｆ、１５…ＣＰＵ、１６…バス、１７…Ｉ／Ｏ、１

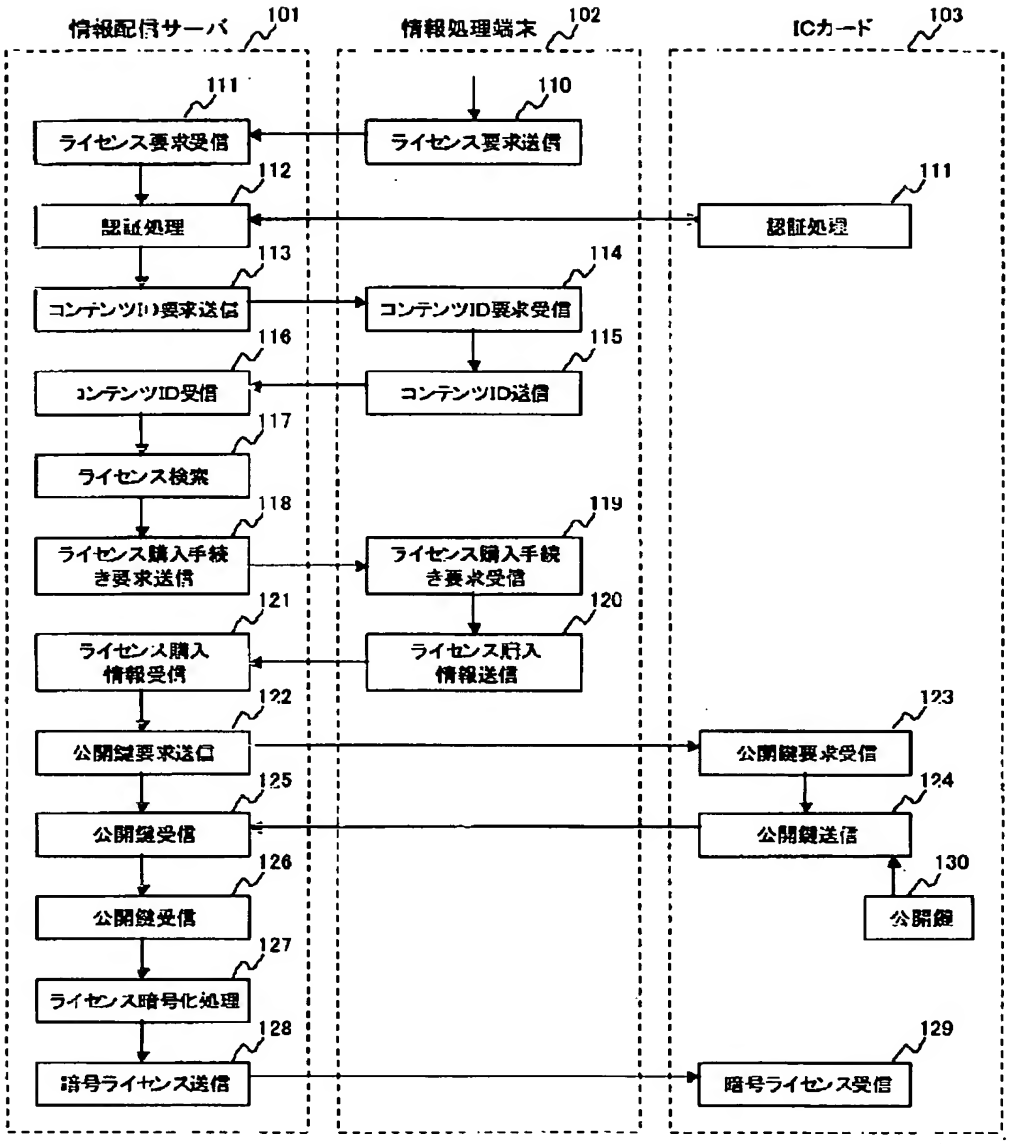
8…入力手段、19…再生手段、35…表示手段、36…音声出力手段、20…ICカード、21…認証手段、22…公開鍵、23…複合化手段、24…秘密鍵、26…暗号手段、27…鍵生成手段、29…鍵記録手段、30…加算手段、31…複合手段

【図1】

[図1]

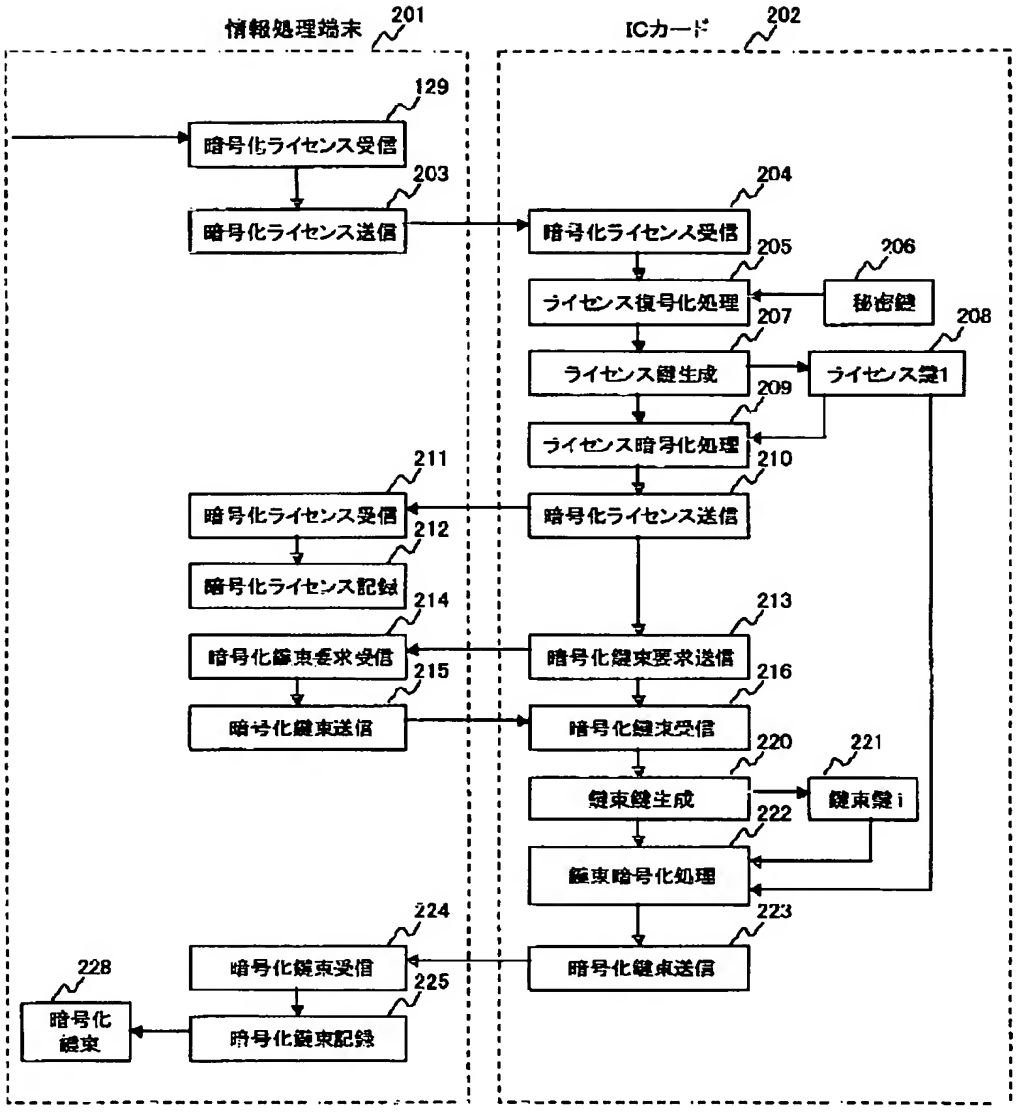


【図2】

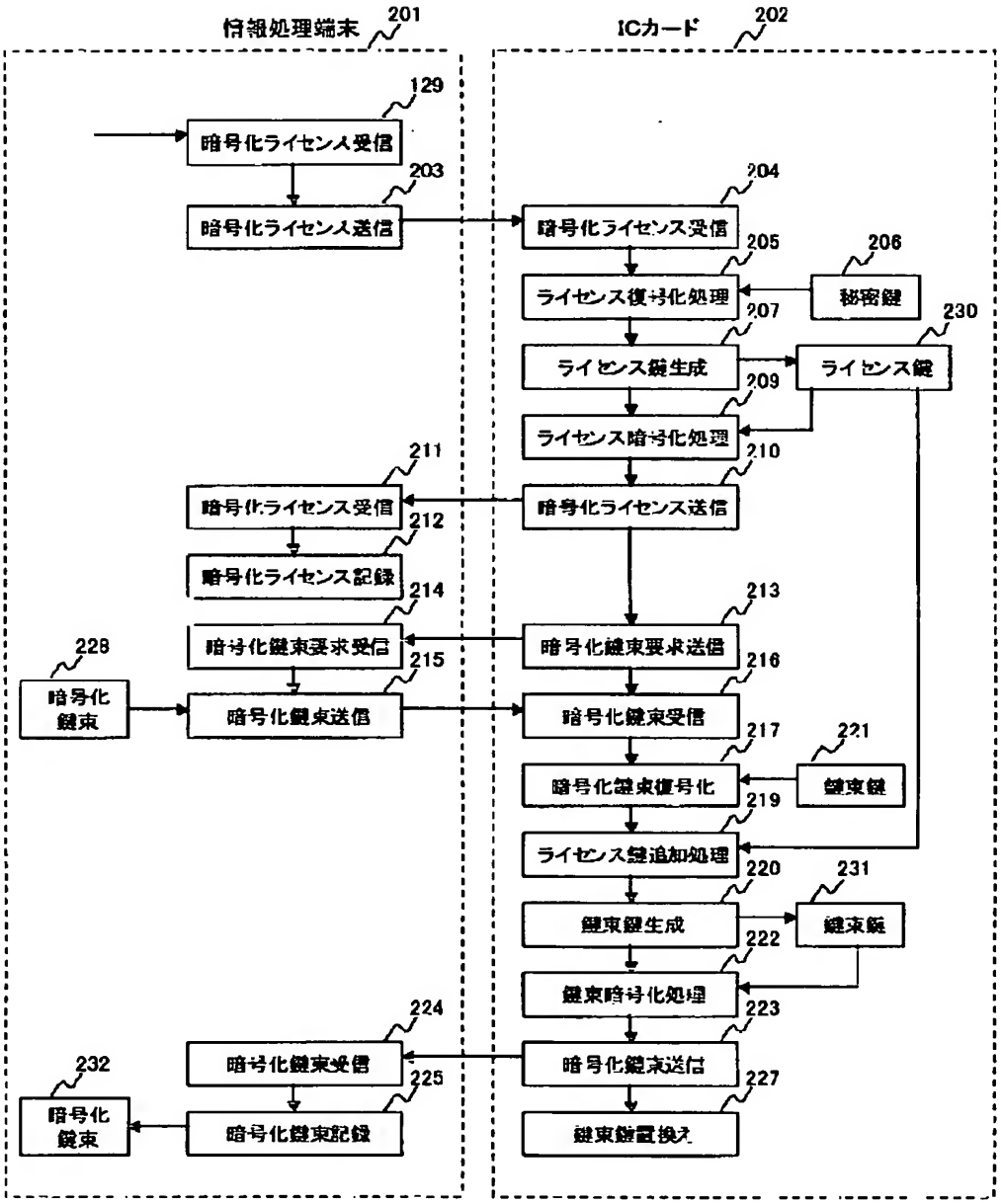

[図2]
情報配信サーバ
101
情報処理端末
102
ICカード
103
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
ライセンス要求送信
ライセンス要求受信
認証処理
認証処理
コンテンツID要求送信
コンテンツID要求受信
コンテンツID送信
コンテンツID受信
ライセンス検索
ライセンス購入手続き要求送信
ライセンス購入手続き要求受信
ライセンス購入情報送信
ライセンス購入情報受信
公開鍵要求送信
公開鍵要求受信
公開鍵送信
公開鍵受信
公開鍵
公開鍵受信
ライセンス暗号化処理
暗号ライセンス送信
暗号ライセンス受信

【図３】

[図３]

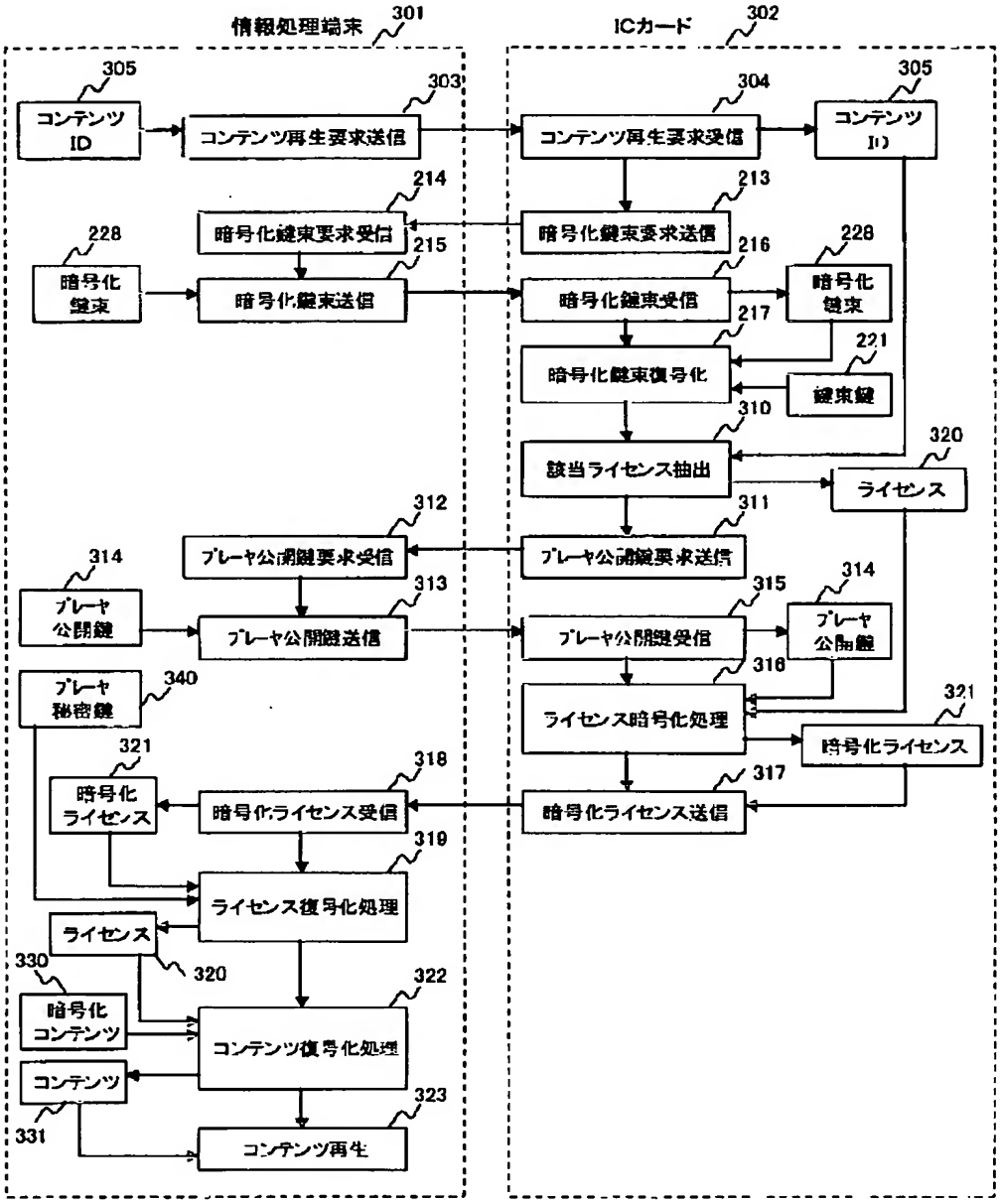

情報処理端末
201
ICカード
202
129
暗号化ライセンス受信
203
暗号化ライセンス送信
204
暗号化ライセンス受信
205
ライセンス復号化処理
206
秘密鍵
207
ライセンス鍵生成
208
ライセンス鍵1
209
ライセンス暗号化処理
210
暗号化ライセンス送信
211
暗号化ライセンス受信
212
暗号化ライセンス記録
213
暗号化鍵束要求送信
214
暗号化鍵束要求受信
215
暗号化鍵束送信
216
暗号化鍵束受信
220
鍵束鍵生成
221
鍵束鍵i
222
鍵束暗号化処理
223
暗号化鍵束送信
224
暗号化鍵束受信
225
暗号化鍵束記録
228
暗号化鍵束

【図4】


情報処理端末
201
ICカード
202
129
暗号化ライセンス受信
203
暗号化ライセンス送信
204
暗号化ライセンス受信
205
ライセンス復号化処理
206
秘密鍵
207
ライセンス鍵生成
230
ライセンス鍵
209
ライセンス暗号化処理
210
暗号化ライセンス送信
211
暗号化ライセンス受信
212
暗号化ライセンス記録
213
暗号化鍵束要求送信
214
暗号化鍵束要求受信
228
暗号化鍵束
215
暗号化鍵束送信
216
暗号化鍵束受信
217
暗号化鍵束復号化
221
鍵束鍵
219
ライセンス鍵追加処理
220
鍵束鍵生成
231
鍵束鍵
222
鍵束暗号化処理
223
暗号化鍵束送信
224
暗号化鍵束受信
232
暗号化鍵束
225
暗号化鍵束記録
227
鍵束鍵置換え

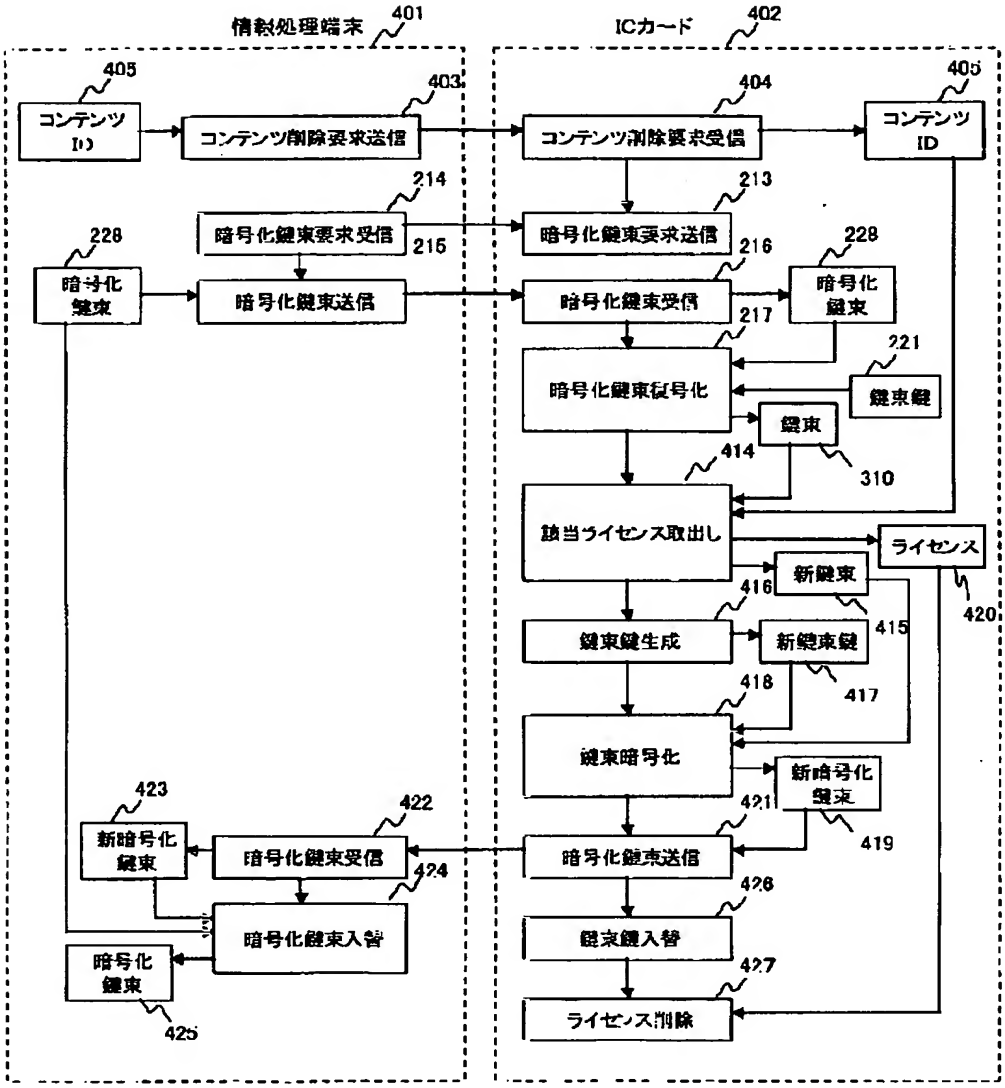
【図５】

[図5]


情報処理端末
301
ICカード
302
305
コンテンツID
303
コンテンツ再生要求送信
304
コンテンツ再生要求受信
305
コンテンツID
214
暗号化鍵束要求受信
213
暗号化鍵束要求送信
228
暗号化鍵束
215
暗号化鍵束送信
216
暗号化鍵束受信
228
暗号化鍵束
217
暗号化鍵束復号化
221
鍵束鍵
310
該当ライセンス抽出
320
ライセンス
312
プレーヤ公開鍵要求受信
311
プレーヤ公開鍵要求送信
314
プレーヤ公開鍵
313
プレーヤ公開鍵送信
315
プレーヤ公開鍵受信
314
プレーヤ公開鍵
340
プレーヤ秘密鍵
316
ライセンス暗号化処理
321
暗号化ライセンス
318
暗号化ライセンス受信
317
暗号化ライセンス送信
321
暗号化ライセンス
319
ライセンス復号化処理
ライセンス
320
330
暗号化コンテンツ
322
コンテンツ復号化処理
コンテンツ
331
323
コンテンツ再生

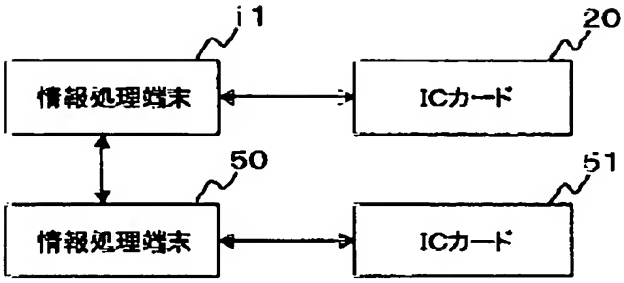
【図6】

【図6】


情報処理端末
401
ICカード
402
405
コンテンツID
403
コンテンツ削除要求送信
404
コンテンツ削除要求受信
405
コンテンツID
214
暗号化鍵束要求受信
215
213
暗号化鍵束要求送信
228
暗号化鍵束
暗号化鍵束送信
216
暗号化鍵束受信
228
暗号化鍵束
217
221
暗号化鍵束復号化
鍵束鍵
鍵束
310
414
該当ライセンス取出し
ライセンス
新鍵束
420
416
鍵束鍵生成
新鍵束鍵
415
417
418
鍵束暗号化
新暗号化鍵束
419
423
新暗号化鍵束
422
暗号化鍵束受信
421
暗号化鍵束送信
424
暗号化鍵束入替
426
鍵束鍵入替
427
ライセンス削除
暗号化鍵束
425

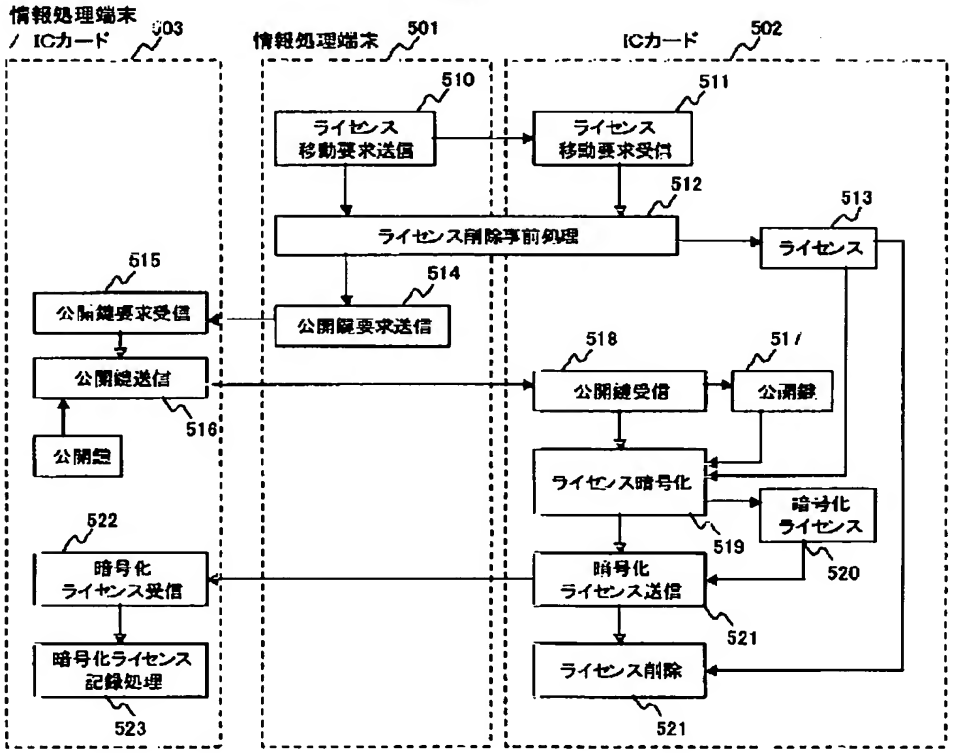
【図7】

[図7]



【図8】

[図8]



フロントページの続き

(51)Int.Cl.⁷	識別記号	FI	(参考)
G06F 17/60	ZEC	G06F 17/60	ZEC
G06K 17/00		G06K 17/00	L
19/00		19/00	Q
H04L 9/08		H04L 9/00	601A

601F

Fターム(参考) 5B017 AA03 AA06 BA07 BA09 CA05
CA14
5B035 AA00 BB09 BC00 CA11
5B058 CA01 KA02 KA04 KA08 KA31
KA35 YA16 YA20
5J104 AA16 AA34 EA04 EA09 JA21
NA02 NA35 NA37 PA07

Japanese Kokai Patent Application No. 2003-216500

Job No.: 228-117010
Ref.: Japanese patent no. JP2003-216500/PU030342 US/PPK(Fidiliz)/Order No. 7780
Translated from Japanese by the McElroy Translation Company
800-531-9977 customerservice@mcelroytranslation.com

JAPANESE PATENT OFFICE
PATENT JOURNAL (A)
KOKAI PATENT APPLICATION NO. P2003-216500A

Int. Cl.[7]:	G 06 F 12/14 17/60 G 06 K 17/00 19/00 H 04 L 9/08
Filing No.:	P2002-13650
Filing Date:	January 23, 2002
Publication Date:	July 31, 2003
No. of Claims:	7 (Total of 14 pages; OL)
Examination Request:	Not filed

DIGITAL COPYRIGHT MANAGEMENT SYSTEM

Inventor:	Mayumi Nakade Manufacturing Technical Research Lab., Hitachi, Ltd. 292 Yoshida-cho, Tozuka-ku, Yokohama-shi
Applicant:	000005108 Hitachi, Ltd. 4-6 Kandasurugadai, Chiyoda-ku, Tokyo
Agent:	100075096 Yasuo Sakuta, patent attorney

[There are no amendments to this patent.]

Abstract

Problems to be solved by the invention

In the digital copyright protection system of the prior art, when the number of purchase licenses is increased, the amount of digital license data managed by a secure card increases, and a larger capacity is needed.

Means to solve the problems

According to the present invention, the plural key data for encrypting plural license data are summarized, and a single item of key-bundle key data is used for encryption. With an IC card, said key bundle data alone are managed, and the encrypted data obtained by summarizing the license encrypted data and the key data used in encryption are stored in the information processor. With said means, it is possible to manage plural licenses by recording a single item of key bundle data in the IC card. Also, the encrypted license and the key bundle are effective only when they are used together with the IC card used in authentication [sic; encryption]*. Consequently, unauthorized use of the license by others is impossible, and only the IC card holder can easily perform copying and reproduction.

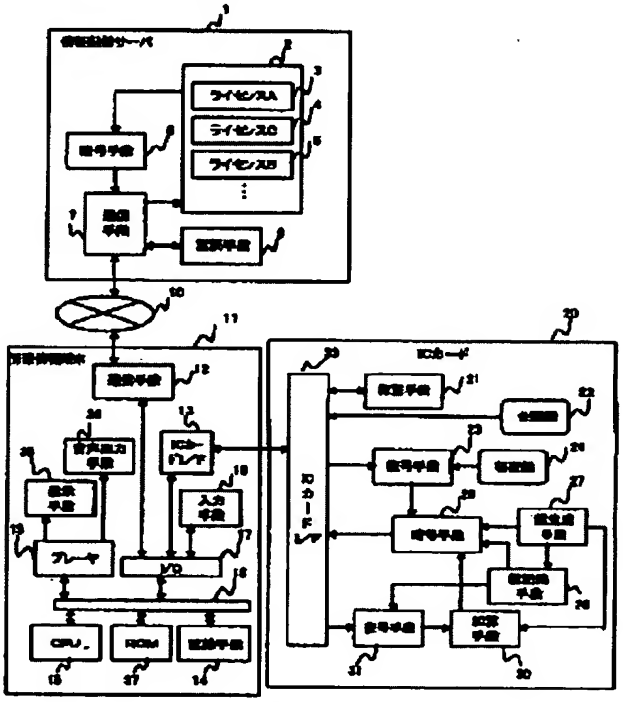


Figure 1

* [Note: This is a typographical error in the original, and is translated as encryption" in several other obvious places in the patent.]

Key:
1 Information distribution service
3 License A
4 License C
5 License B
6 Encryption means
7 Communication means
8 Authentication means
11 Information information terminal [sic, Information processing terminal]
12 Communication means
13 IC card I/F
14 Recording means
18 Input means
19 Player
20 IC card
21 Authentication means
22 Public key
23 Decoding means
24 Private key
26 Encryption means
27 Key generating means
29 Key recording means
30 Adding means
31 Decoding means
35 Display means
36 Sound output means
33 IC card I/F

Claims

1. A type of digital copyright management system characterized by the following facts:

The digital copyright management system comprises an IC card, on which the private key and the public key corresponding to the private key are recorded, an information processor having a connection means to said IC card and a data communication means, and a license delivery device, which stores plural license data and delivers the license data via said communication means to said information processor;

said license delivery device has a first encryption means, which encrypts the license data by means of the public key of said IC card and takes them as the first encrypted license data, and a license delivery means, which delivers said first encrypted license data to said information processor; said information processing terminal transfers the first encrypted license data delivered by said license delivery device to said IC card; said IC card has a decoding means, which decodes the first encrypted license data delivered from said license delivery device with

said private key to form license data, a key data generating means that generates the key data for each said license data, a second encryption means, which makes use of said key data to encrypt said license data to generate the second encrypted license data, and a key bundle data generating means, which summarizes said key data for each said license data to form a single key bundle data;

by means of said second encryption means, which makes use of said key data generating means to generate key-bundle key data for each said prepared key bundle data, and with said key-bundle key data as the key data, said system encrypts said key bundle data to generate said encrypted key bundle data, and records said key-bundle key data on the IC card.

2. The digital copyright management system described in Claim 1 characterized by the fact that

the second encrypted license data and said encrypted key bundle data generated by said second encryption means of said IC card are recorded in said information processor.

3. The digital copyright management system described in Claim 1 or 2 characterized by the following facts:

a second compounding [sic; decoding]* means that decodes said encrypted key bundle data to said key-bundle key data is set in said IC card;

each time that said IC card receives said second encrypted license data from said information processor, said key-bundle key data are used to generate the new key data and the new key-bundle key data by means of said key bundle data said key generating means [sic; said key bundle data generating key generating means], and the newly generated key data are added to the key bundle data by said key bundle data generating means to generate the new key bundle data; by means of said new key-bundle key data, the new key bundle data are encrypted by said second encryption means to generate the new encrypted key bundle data, and said key-bundle key data are recorded in the IC card, while said key-bundle key data are deleted as old key-bundle key data from the records.

4. The digital copyright management system described in Claim 1, 2 or 3 characterized by the following facts: according to the license data deletion request or movement request from said information processor, said IC card makes use of said key-bundle key data to decode said encrypted key bundle data by said decoding means to form the key bundle data; the key data corresponding to the license data for which said deletion request or movement request was made are deleted from said key data to form the new key bundle data; said key generation means is used to generate new key-bundle key data; the new key-bundle key data are used to encrypt said

---

* [Note: This is a typographical error in the original and has been translated as "decoding" where it appears elsewhere in the patent.]

new key bundle data by means of said second encryption means, and the new encrypted key bundle data are recorded in said information processor; said new key-bundle key data are recorded in said IC card, and at the same time, said old key-bundle key data are deleted.

5. The digital copyright management system described in Claim 1, 2, 3 or 4 characterized by the following facts:

it has a third encryption means, which encrypts the data by means of the public key in said IC card;

and when the license data are moved to a second information processor, said moved license data are encrypted by said third encryption means using the public key of the second IC card connected to said second information processor.

6. A type of IC card characterized by the following facts: it has the following parts: a private key, a public key corresponding to said private key, a decoding means that uses said private key to decode the encrypted data encrypted by means of said public key to access a data item, a key data generating means that generates the key data for each said data item, an encryption means that encrypts said license data with said key data to generate the second encrypted data, and a key bundle data generating means that summarizes said key data for each said data item to form a key bundle data item; with said key data generating means, the key-bundle key data are generated for each said prepared key bundle data item; with said key-bundle key data as the key data, said second encryption means is used to encrypt said key bundle data to generate encrypted key bundle data; and said key-bundle key data are recorded on the IC card.

7. A digital copyright management method characterized by the following facts: the IC card has a private key, a public key corresponding to said private key, a decoding means that uses said private key to decode the encrypted data encrypted by said public key to get the data item, a key data generating means that generates the key data for each said data item, an encryption means that encrypts said license data with said key data to generate the second encrypted data, and a key bundle data generating means that summarizes said key data for each said data item to form a key bundle data; with said key data generating means, the key-bundle key data are generated for each said prepared key bundle data; with said key-bundle key data as the key data, said second encryption means is used to encrypt said key bundle data to generate encrypted key bundle data; and said key-bundle key data are recorded in the IC card; said second encrypted license data and said encrypted key bundle data are recorded in the information processor having a connecting means with said IC card.

Detailed explanation of the invention

[0001]

Technical field of the invention

The present invention pertains to a type of digital copyright management system for protecting the copyright of digitized moving pictures, sound, and other content. In particular, the present invention pertains to a type of digital copyright management system that makes use of an IC card to protect the copyright.

[0002]

Prior art

The Keitaide Music content delivery service standardized by the Keitaide Music Consortium uses a conventional system for protecting the digital copyright of the content of digitized moving pictures, sound, and other content in the prior art.

[0003]

According to said Keitaide Music, the encrypted contents are delivered free of charge from a content server via cell phone network. As for the license that is the key for decoding the encrypted content, the encrypted license is delivered via the cell phone network from the license server when the user purchases the right of the license. The delivered encrypted license is input via the cell phone to a secure memory card, and it is decoded and stored there. When the content is to be reproduced by a player, the encrypted content and license are accessed from said memory card, and the encrypted content is decoded for reproduction by means of the license.

[0004]

Problems to be solved by the invention

Because the license is entirely stored in the memory card in said copyright protection system of the present invention, the number of the licenses that can be stored is restricted according to the capacity of the memory card. In particular, for an IC card with a relatively low capacity, plural memory cards would be needed if a lot of licenses were purchased. Also, no consideration is given in said prior art license transfers to other persons, so that the system is not very convenient for the user.

[0005]

The purpose of the present invention is to provide a type of digital copyright management system characterized by the fact that more licenses can be managed relative to the storage capacity of an IC card, such as low-recording-capacity IC cards that can be carried around easily,

safe management of the encrypted licenses is possible, and the owner of the IC card can copy the encrypted licenses to plural devices he/she owns, so that the owner needs only to carry around the IC card, while reproduction of the content can be performed anywhere.

[0006]

Means to solve the problems

In order to solve the aforementioned problems, the present invention provides a type of digital copyright management system. As one characteristic feature of the digital copyright management system of the present invention, when a license is purchased, the encrypted license received from the server is decoded by means of the private key in the IC card; a random number generating means is then used to generate a new license key, and the license decoded by means of said license key is encrypted again, and the encrypted license is stored in the information processing terminal. When plural licenses are to be held, a license key bundle key is generated in the IC card; said plural license keys are encrypted as a group, and the bundled encrypted license keys are stored at the information processing terminal. The license key bundle key is stored in the IC card.

[0007]

By means of said license storage method, it is possible to manage more licenses even when using an IC card with a relatively low storage capacity.

[0008]

Embodiment of the invention

In the following, application examples of the present invention with reference to figures will be explained.

[0009]

Figure 1 is a functional block diagram illustrating the digital copyright management system in Application Example 1 of the present invention. Here, (1) represents an information delivery server; (10) represents a network, (11) represents an information processing terminal, and (20) represents an IC card. Said information delivery server (1) and information processing terminal (11) are connected by means of network (7) [sic; 10]*, and IC card (20) is connected to information processing terminal (11). In the following, their constitutions will be explained.

---

* [Note: This is one of numerous numbering errors in the text and figures.]

[0010]

Said information delivery server (1) has at least recording means (2), encryption means (6), authentication means (8), and communication means (7). According to a request received by communication means (7), said information delivery server (1) performs authentication of the IC card with authentication means (8), encryption of the license stored in recording means (2) with encryption means (6), and transmission of the encrypted license via communication means (7).

[0011]

Said information processing terminal (11) has at least CPU (15), ROM (37) connected to CPU (15) with bus (16), recording means (14), I/O [input/output] (17), reproduction means (19), input means (18) controlled by I/O (17), IC card I/F [interface] (13), communication means (12), display device (35), and sound output means (36). Said recording means (12)[sic; (2)] may be a rewritable RAM, hard disk, or flash ROM. Said input means may be operating buttons or a touch panel, or the like. Said IC card I/F (13) is connected to IC card (20), and communication means (12) is connected with information delivery server (1) by means of network (10).

[0012]

Said IC card (20) has at least the following parts: input/output I/F (23) for connection to information processing terminal (11), authentication means (21) for authentication of information delivery server (1), public key (22) for encrypting the license by encryption means (6) of information delivery server (1), private key (24) corresponding to said public key (22), decoding means (23) for decoding the encrypted license using private key (24), key generating means (27) for generating plural key data, encryption means (26) for encrypting the data with the key data generated by key generating means (27), adding means (30) that summarizes some of the key data generated with key generating means (27) to form key bundle data, key recording means (29), which records the key-bundle key data when said key bundle data are encrypted, key bundle data call means (40) that calls the encrypted key bundle data from recording means (14) of information terminal (11), and decoding means (31) that decodes the input data with the key-bundle key data recorded in the key recording means.

[0013]

In the following, the procedure from the request for a license in the copyright management system shown in Figure 1 to procurement of the license by the IC card will be explained with reference to Figure 2.

[0014]

Figure 2 is a flow chart for the license procurement processing in Application Example 1. Here, (101), (102), (103) indicate the processing performed in information delivery server (1), information terminal (5) [sic; (11)], and IC card (20) shown in Figure 1, respectively.

[0015]

When a license is to be procured, the user uses input means (18) of information terminal (1) [sic; (11)] shown in Figure 1 to express the intention to request a license, and as a result, information terminal (1) sends the license request to information delivery server (1). Here, information delivery server (1), which performs license request reception (111), performs authentication processing (112) of IC card (20), and the same authentication processing (130) of information delivery server (1) is also performed in IC card (20). Specific examples of authentication processing (112) and authentication processing (130) will be presented later.

[0016]

After authentication processing (112) is complete, information delivery server (1) performs content ID request transmission (113) at information processing terminal (5). Here, as shown in Figure 2, content ID is taken as the data requested by information delivery server (1). However, it may also be the content name or other data that can specify the content. Said information processing terminal (5), which performs content ID request reception (114), performs content ID transmission (115) once the requested content is determined. Here, instead of content ID request transmission (113), information delivery server (1) can also send the list of contents, which is used by the information delivery server in managing the license, to the information processing terminal. A scheme can also be adopted in which the user selects the content from the list of contents when the list of contents is sent. In this case, the list of contents is displayed on display device (35) at information processing terminal (5), and the user is prompted to specify the desired content. As a result, the user uses input means (18) to specify the content from the input data, and performs content ID transmission (115) to information delivery server (1). Said information delivery server (1), which performed content ID reception (116), performs license searching (117) from the content ID, accesses the license data, and uses public key (22) of IC card (9) [sic] to perform license encryption processing. After the encrypted license is received by information processing terminal (5), it is sent to IC card (20).

[0017]

In the following, the procedure of encrypted license recording in information processing terminal (5) and IC card (9) will be explained with reference to Figures 3 and 4.

[0018]

Figure 3 is a flow chart illustrating the license recording processing in Application Example 1 of the present invention for a license that is procured for the first time.

[0019]

The same part numbers as those adopted in Figure 2 are adopted here. After information terminal (11) performs encrypted license reception (129), instead of recording it in recording means (14) of information terminal (11), encrypted license transmission (203) to IC card (20) is performed. After the IC card performs encrypted license reception (204), it performs license decoding processing (205) by means of private key (206) corresponding to public key (130), and it performs decoding of the encrypted license. IC card (20) then uses key generating means (27) to perform license key generation (207), and in license encryption processing (209), license key (208) is generated for each license. By means of said license key (208), the license that has been decoded in the former stage by encryption means (26) is re-encrypted. Then, encrypted license transmission (210) is performed. After performing encrypted license reception (211) at information processing terminal (11) encrypted license recording (212) is performed, and said encrypted license encrypted by a different license key for each license is recorded in the recording means of information processing terminal (11).

[0020]

After performing encrypted license transmission (210), said IC card (20) requests the encrypted key bundle, which has plural license keys (208) summarized by adding means (30) and encrypted by encryption means (26), from information processing terminal (11) by means of encrypted key bundle request transmission (213). After portable information terminal (201) performs reception (214) of the encrypted key bundle request, because there is as yet no encrypted key bundle, the encrypted key bundle portion performs empty encrypted key bundle transmission (215). When said empty encrypted key bundle reception (216) is performed, IC card (20) performs key bundle generation (220) that generates the key for the key bundle. At this time, generated key bundle key (a221) is recorded by key recording means (29) of the IC card in IC card (20). Then IC card (20) uses key bundle key (a221) to perform key bundle encryption processing (222) that encrypts license key (208). Here, the encrypted license key performs encrypted key bundle transmission processing (223) that sends the encrypted license key as the encrypted key bundle to information processing terminal (11). At information processing terminal (11), after the encrypted key bundle is received from IC card (20) by means of

encrypted key bundle reception (224), encrypted key bundle recording (225) is performed to record the encrypted key bundle in recording means (14).

[0021]

In the above, an explanation has been provided for license recording processing when the license is procured for the first time. First of all, whether the license is being procured for the first time or no license is recorded at information processing terminal (5) is checked on the side of IC card (20), from the fact that no key-bundle key is recorded in IC card (20), said encrypted key bundle request transmission (213) from IC card (20), can be omitted together with empty encrypted key bundle reception (216).

[0022]

In the following, a case in which the license is already recorded at information processing terminal (5) will be explained with reference to Figure 4. Figure 4 is a flow chart of the license recording processing in Application Example 1. The same part numbers as those adopted above in Figure 3 are adopted here, and because the process up to the step encrypted key bundle transmission (214) of information processing terminal (5) is the same as in Figure 3, it will not be explained in detail again. According to the present invention, because a license key is generated for each license, license key (208) in Figure 3 and license key (230) shown in Figure 4 are keys of different data.

[0023]

Said information processing terminal (5) performs encrypted key bundle transmission (228) [sic; (215)], in which encrypted key bundle (228) that has been recorded is transmitted to the IC card. Said IC card (20) uses decoding means (31) to perform encrypted key bundle decoding (217), the processing for decoding encrypted key bundle (228) received via encrypted key bundle reception (216), using key-bundle key (221), and performs license key addition processing (219) in which license key (230) is added by adding means (30) to the decoded key bundle. In addition, IC card (20) uses key generating means (27) to generate the new key-bundle key, key-bundle key generation processing (222) is performed to generate key-bundle key (231). Also, according to the present invention, the key-bundle key is newly generated for each new key bundle, and key-bundle key (221) and key-bundle key (231) are constituted of different data.

[0024]

In said IC card (20), by means of key-bundle key (231) newly formed by encryption means (26), key-bundle key generation processing (222) is performed to encrypt the newly

formed key bundle, followed by encrypted key bundle transmission (224) to information processing terminal (5). In information processing terminal (5), encrypted key bundle reception (224) is performed to receive the new encrypted key bundle, and the encrypted key bundle is recorded for new encrypted key bundle (232) instead of encrypted key bundle (228). After encrypted key bundle transmission processing (223) is performed in IC card (20), old key-bundle key (221) is discarded, and new key-bundle key (231) is recorded as key-bundle key (221).

[0025]

In the above, the license recording method according to the present invention has been explained. According to the recording method of the present invention, because the license is encrypted by different keys, even when one key is broken, a hacker still cannot take out the licenses. Also, because what is recorded in the IC card is at least one key-bundle key, it is possible to construct a system many licenses can be managed even in an IC card with relatively low capacity.

[0026]

The reproduction of content will be explained in the following. Figure 5 shows an example of the flow of the content reproduction processing in Application Example 1 of the present invention.

[0027]

According to a content reproduction command from the user, information processing terminal (5) performs content reproduction request transmission (303) that starts the processing for reproduction of the content together with content ID (305) in IC card (20). A scheme can also be adopted in which transmission is performed later for content ID (305). In order to fetch the license needed for content reproduction when IC card (20) receives content reproduction request (304), encrypted key bundle request transmission (213) is performed at information processing terminal (5) to obtain encrypted key bundle (228). When information processing terminal (5) performs encrypted key bundle reception (214), encrypted key bundle transmission (215) is performed to send encrypted key bundle (228) to IC card (20). Also, a message of response saying that preparation for the content reproduction processing is ready may be sufficient as encrypted key bundle request transmission (213). When IC card (20) performs encrypted key bundle reception (216), encrypted key bundle decoding (217) is performed as the decoding processing using key-bundle key (221) having encrypted key bundle (228) recorded in key recording means (29), and license extraction (310) from the decoded key bundle is performed to fetch license (320) corresponding to procured content ID (305) from the decoded key bundle. IC

card (20) then prepares to perform transmission of the license. First of all, in order to encrypt the license, player public key request transmission (311) is performed. After performing player public key request reception (312), information processing terminal (11) performs player public key transmission (313) to send player public key (314) to IC card (20). Said IC card (20) that performs player public key reception (315) performs license encryption processing (316) to encrypt license (320) that has been decoded by means of player public key (314), and performs encrypted license transmission to transmit encrypted license (321) to the information processing terminal. Said information processing terminal (11) that performs encrypted license reception (318) performs license decoding processing (319) with the encrypted license decoded by player private key (340) corresponding to player public key (314), so as to fetch license (320). It then performs content decoding processing (322) to decode encrypted content (330) with license (320), and it fetches content (331), followed by content reproduction (323), to convert content (331) to sounds or images.

[0028]

As explained above, according to the present invention, the license is stored in information processing terminal (11) instead of in the IC card. Consequently, only the key that summarizes the licenses is stored in the IC card. Consequently, the licenses are managed irrespective of the capacity of the IC card. Also, because the license is encrypted by a different key for each license, even when a hacker discovers one key, he/she can still not decode all of the keys. In addition, because the key is changed each time of encryption, a safe system can be formed.

[0029]

In the following, a case in which a license is to be deleted will be explained with reference to Figure 6.

[0030]

Figure 6 is a flow chart illustrating an example of the license deletion processing for the digital copyright management system in Application Example 1 of the present invention. Here, (401) represents the processing at the information processing terminal, and (402) represents the processing within IC card (20). The same part numbers as those adopted above for Figure 4 are adopted here, and they will not be explained again.

[0031]

When the user makes use of input means (18) to input a command for content deletion or content movement, together with deletion content ID (405), at information processing terminal (11), content deletion request transmission (403) is performed. In IC card (20) that has received the content deletion request, encrypted key bundle request transmission (213) to information processing terminal (11) is performed. Then, just as in the process shown in Figure 4, encrypted key bundle reception (214) and encrypted key bundle transmission (215) in information processing terminal (11), and encrypted key bundle reception (216) and encrypted key bundle decoding (217) at IC card (20) are performed. Then, in IC card (20), the license corresponding to deletion content ID (405) is fetched from the bundle of the encrypted license as a key bundle, and key bundle generation (416) for generating a new key-bundle key for bundling the remaining licenses as a new key bundle is performed. Then, key bundle encryption processing (418) that encrypts the new key bundle by new key-bundle key (417) is performed to generate new encrypted key bundle (419) and to perform encrypted key bundle transmission (421). In IC card (20), after encrypted key bundle transmission (421) is performed, key-bundle key replacement (426) is performed for using new key-bundle key (417) to replace key-bundle key (221), and the fetched license is deleted. After performing encrypted key bundle reception (422), information processing terminal (11) performs encrypted key bundle replacement (424) using new encrypted key bundle (423) to replace encrypted key bundle (228).

[0032]

By means of the aforementioned license deletion system, the license to be deleted is processed and deleted in the IC card, so that the user cannot make unauthorized use of the license. Also, a new key-bundle key is formed, and only the new key bundle is effective, so that even when the old key bundle is copied, it still cannot be used. Consequently, complete deletion of the license is performed. Also, by copying the new key bundle, an effective IC card can be gained, so that the license can be made effective at other information processing terminals. This makes the system user-friendly.

[0033]

In the following, transfer of a license to another person will be explained with reference to Figures 7 and 8.

[0034]

Figure 7 is a diagram illustrating an example of the constitution involved when a license is to be transferred in Application Example 1 of the present invention.

[0035]

Said information processing terminal (11) and IC card (20) are the same as those explained with reference to Figure 1. Information processing terminal (50) has the same function as that of information processing terminal (11), and IC card (51) has the same function as that of IC card (20). Said information processing terminal (11) and information processing terminal (50) are connected using various communication means in either a wireless or wired way to perform data exchange. In the following, the processing for license transfer with reference to Figure 8 will be explained.

[0036]

Figure 8 is a diagram illustrating the processing flow for transfer of a license to the copyright management system of the present invention. The processing performed at information processing terminal (11) on the side that transfers the license is indicated by (501), the processing in IC card (20) is indicated by (502), and the processing of information processing terminal (50) and IC card (51) on the side that receives the license is indicated by (503).

[0037]

Upon input from the user, information processing terminal (11) performs license transfer request (510), and IC card (20) performs license request reception (511), whereupon, license deletion processing (512) explained with reference to Figure 6 is performed by information processing terminal (11) and IC card (20). However, the processing of license deletion (427) is not performed immediately. Said information processing terminal (11) performs public key request transmission (514) to information processing terminal (50). Said information processing terminal (50) that has performed public key request reception (515) performs public key transmission (516), and sends public key (517) recorded in IC card (51). After reception of the public [key], information processing terminal (11) sends the public key to IC card (20) as is. Said IC card (20), which has performed public key reception (518), uses the received public key (517) to perform license encryption (521) that encrypts fetched license (513), and performs encrypted license transmission (521). Also, after IC card (20) performs encrypted license transmission (521), it performs license deletion (52) for the transmitted license. Said information processing terminal (11) transmits encrypted license (520) received from IC card (20) as is to information processing terminal (50). Said information processing terminal (50) that has performed encrypted license reception (522) sends encrypted license (520) to IC card (51), and encrypted license recording processing (523) is performed in information processing terminal (50) and IC card

(51). Here, because encrypted license recording processing (523) is identical to the processing explained with reference to Figure 2 or Figure 3, it will not be explained in detail again.

[0038]

As explained above, in the copyright management system of the present invention, the license is encrypted in the IC card by means of the public key of the IC card that performs a transfer, and it is then transmitted. Consequently, the content of the license is not available without the IC card of the transfer receiver, so that the license can be transmitted safely. Also, just as was the case in the explanation of license deletion, the key-bundle key is changed each time the license is moved. This makes unauthorized use of the license difficult.

[0039]

Effect of the invention

As explained above, according to the digital copyright management system of the present invention, many licenses can be managed relative to the storage capacity of an IC card, such as a portable IC card with a fairly small storage capacity. Also, the encrypted data recorded at the portable information terminal can be decoded only by the IC card that generates the key, so that the encrypted license can be managed safely. In addition, the owner of the IC card can copy the encrypted licenses to all of the plural devices possessed by said owner, so that he/she needs to keep only the IC card, and can perform playback of the content anywhere.

Brief description of the figures

Figure 1 is a block diagram illustrating the function of the digital copyright management system in Application Example 1 of the present invention.

Figure 2 is a flow chart illustrating the license procurement processing in Application Example 1 of the present invention.

Figure 3 is a flow chart illustrating the recording processing for a license procured for the first time in Application Example 1 of the present invention.

Figure 4 is a flow chart illustrating the license recording processing in Application Example 1.

Figure 5 is a diagram illustrating an example of the content reproduction processing in Application Example 1 of the present invention.

Figure 6 is a diagram illustrating an example of the flow of license deletion processing in Application Example 1 of the present invention.

Figure 7 is a diagram illustrating an example of the constitution involved in the event of license transfer in Application Example 1 of the present invention.

Figure 8 is a diagram illustrating an example of the constitution [sic; processing flow] involved in the event of license transfer in Application Example 1 of the present invention.

Explanation of symbols

1 Information delivery server
6 Encryption means
7 Communication means
10 Public network
11 Information processing terminal
13 IC card I/F
15 CPU
16 Bus
17 I/O
18 Input means
19 Reproduction means
20 IC card
21 Authentication means
22 Public key
23 Decoding means
24 Private key
26 Encryption means
27 Key generating means
29 Key recording means
30 Adding means
31 Decoding means
35 Display device
36 Sound output means

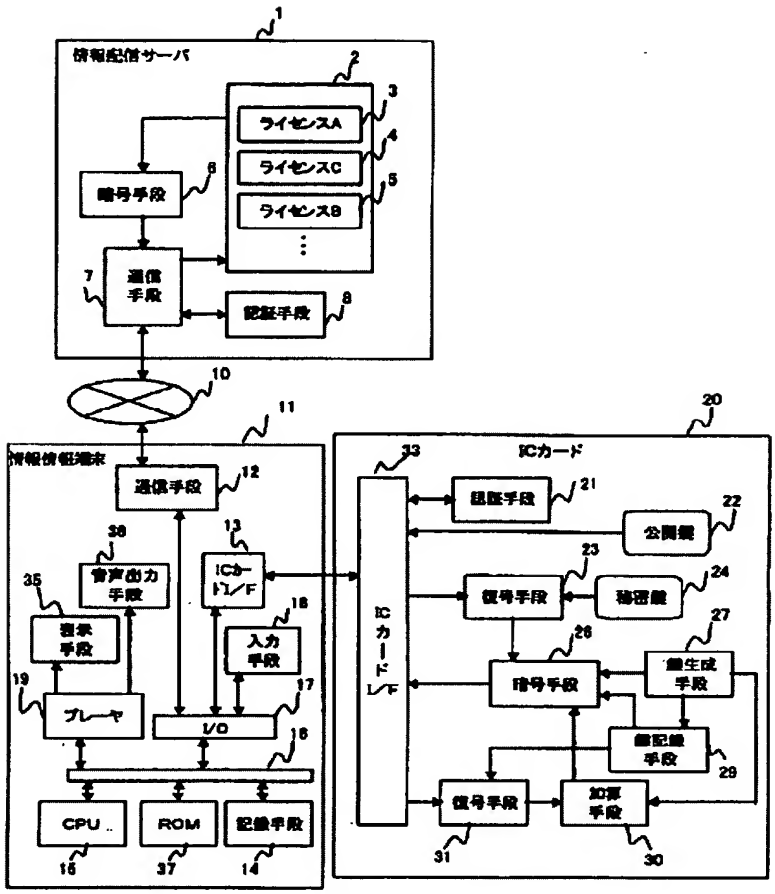


Figure 1

Key:
1 Information distribution service
3 License A
4 License C
5 License B
6 Encryption means
7 Communication means
8 Authentication means
11 Information information terminal [sic, Information processing terminal]
12 Communication means
13 IC card I/F
14 Recording means
18 Input means
19 Player
20 IC card
21 Authentication means
22 Public key

23 Decoding means
24 Private key
26 Encryption means
27 Key generating means
29 Key recording means
30 Adding means
31 Decoding means
35 Display means
36 Sound output means
33 IC card I/F

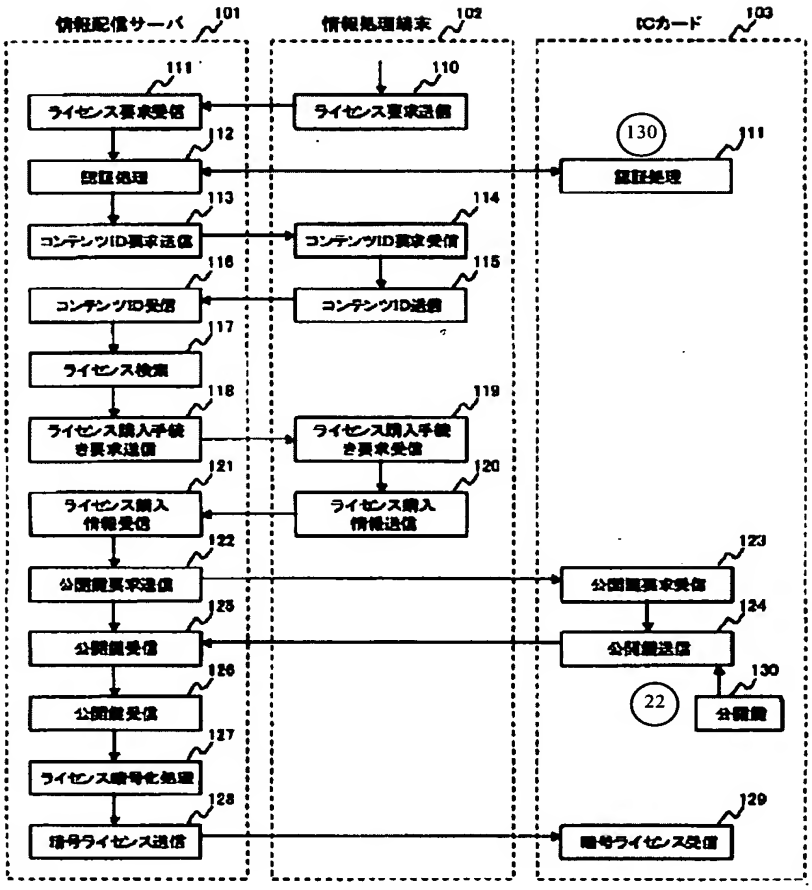


Figure 2

Key: 22 Public key [labeled 130 in figure, but 22 in text]
101 Information delivery server
102 Information processing terminal
103 IC card
110 License request transmission
111 License request reception

112 Authentication processing
113 Content ID request transmission
114 Content ID request reception
115 Content ID transmission
116 Content ID reception
117 License searching
118 License purchase procedure request transmission
119 License purchase procedure request reception
120 License purchase information transmission
121 License purchase information reception
122 Public key request transmission
123 Public key request reception
124 Public key transmission
125 Public key reception
126 Public key reception
127 License encryption processing
128 Encrypted license transmission
129 Encrypted license reception
130 Authentication processing [labeled 111 in figure, but 130 in text]

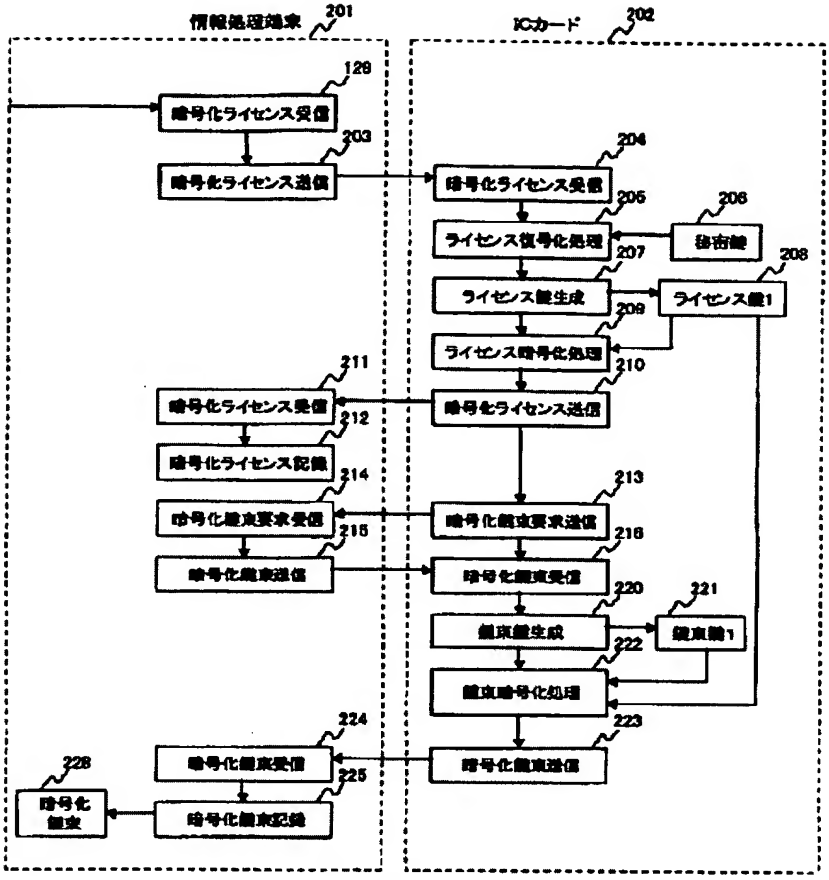


Figure 3

Key:
129 Encrypted license reception
201 Information processing terminal
202 IC card
203 Encrypted license transmission
204 Encrypted license reception
205 License decoding processing
206 Private key
207 License key generation
208 License key 1
209 License encryption processing
210 Encrypted license transmission
211 Encrypted license reception
212 Encrypted license recording
213 Encrypted key bundle request transmission
214 Encrypted key bundle request reception
215 Encrypted key bundle transmission

216 Encrypted key bundle reception
220 Key bundle generation
221 Key-bundle key 1
222 Key-bundle key generation processing
223 Encrypted key bundle transmission processing
224 Encrypted key bundle reception
225 Encrypted key bundle recording
228 Encrypted key bundle

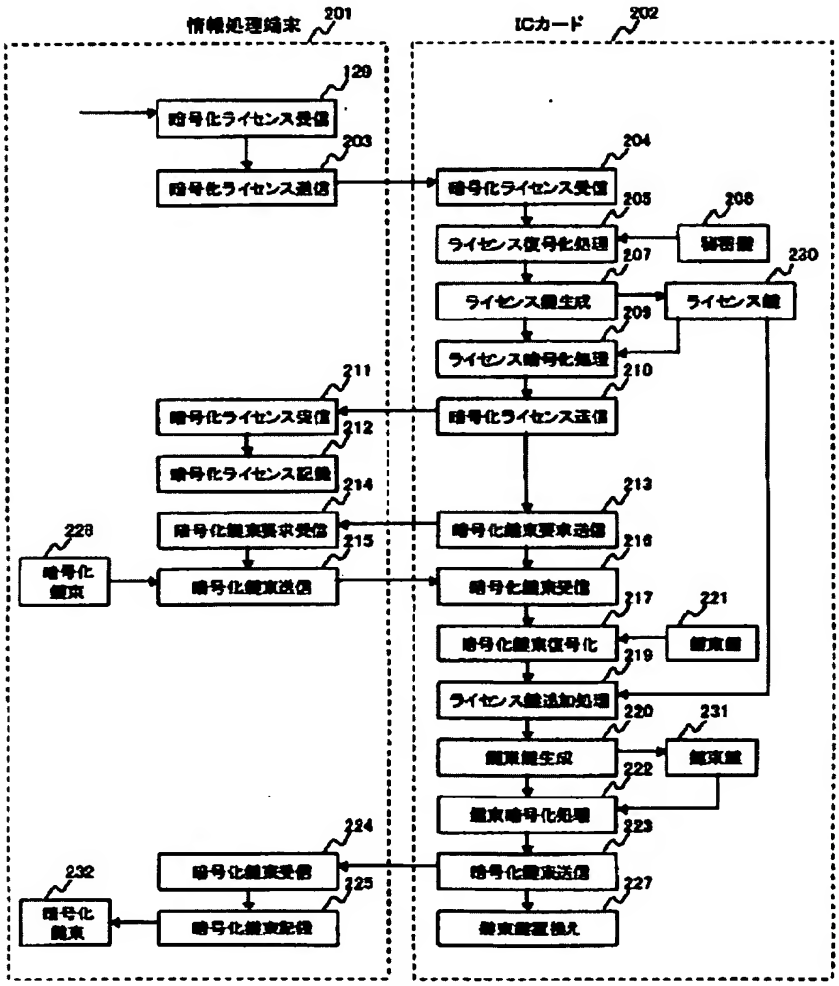


Figure 4

Key: 129 Encrypted license reception
201 Information processing terminal
202 IC card
203 Encrypted license transmission

204 Encrypted license reception
205 License decoding processing
206 Private key
207 License key generation
209 License encryption processing
210 Encrypted license transmission
211 Encrypted license reception
212 Encrypted license recording
213 Encrypted key bundle request transmission
214 Encrypted key bundle request reception
215 Encrypted key bundle transmission
216 Encrypted key bundle reception
217 Encrypted key bundle decoding
219 License key addition processing
220 Key bundle generation
221 Key-bundle key
222 Key-bundle key generation processing
223 Encrypted key bundle transmission processing
224 Encrypted key bundle reception
225 Encrypted key bundle recording
227 Key-bundle key replacement
228 Encrypted key bundle
230 License key
231 Key-bundle key
232 Encrypted key bundle

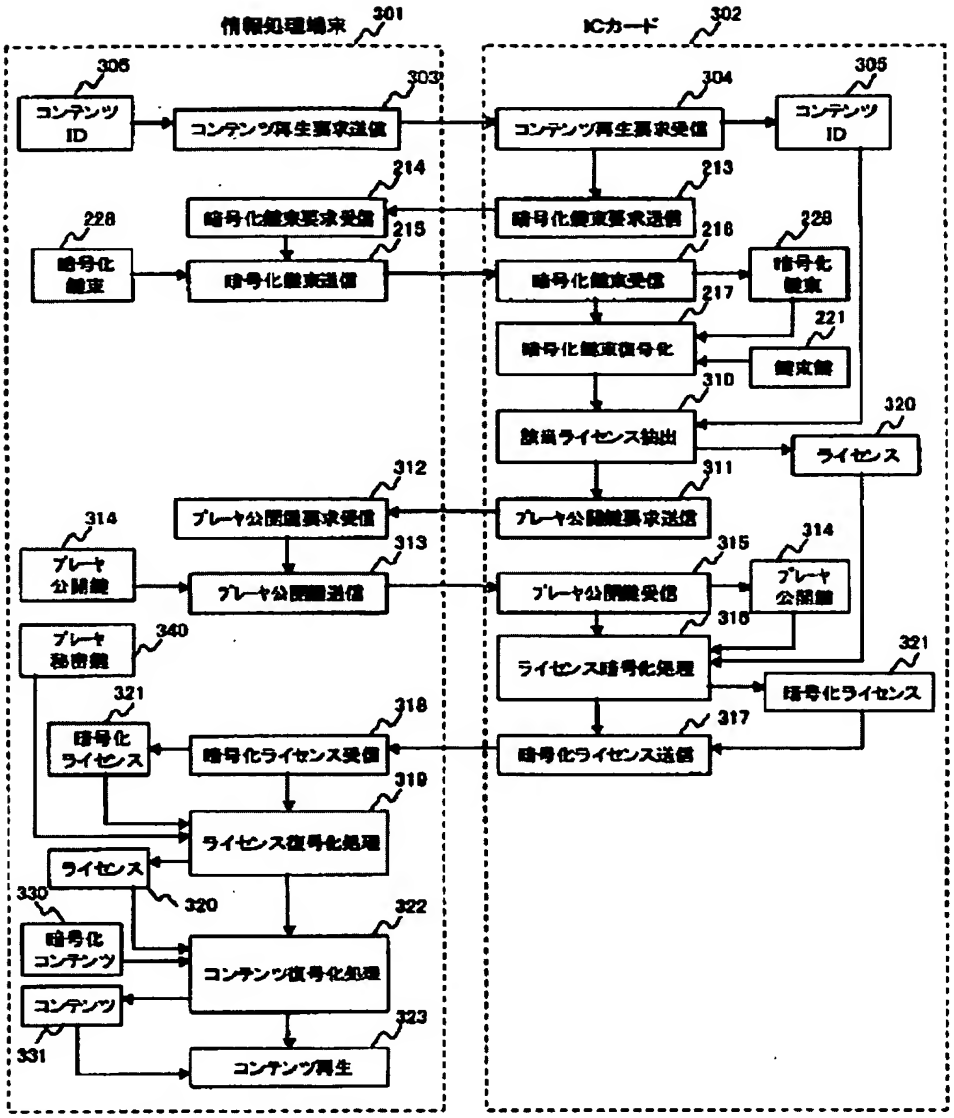


Figure 5

Key:
213 Encrypted key bundle request transmission
214 Encrypted key bundle request reception
215 Encrypted key bundle transmission
216 Encrypted key bundle reception
217 Encrypted key bundle decoding
221 Key-bundle key
228 Encrypted key bundle
301 Information processing terminal
302 IC card

303 Content reproduction request transmission
304 Content reproduction request reception
305 Content ID
310 License extraction
311 Player public key request transmission
312 Player public key request reception
313 Player public key transmission
314 Player public key
315 Player public key reception
316 License encryption processing
317 Encrypted license transmission
318 Encrypted license reception
319 License decoding processing
320 License
321 Encrypted license
322 Content decoding processing
323 Content reproduction
330 Encrypted content
331 Content
340 Player private key

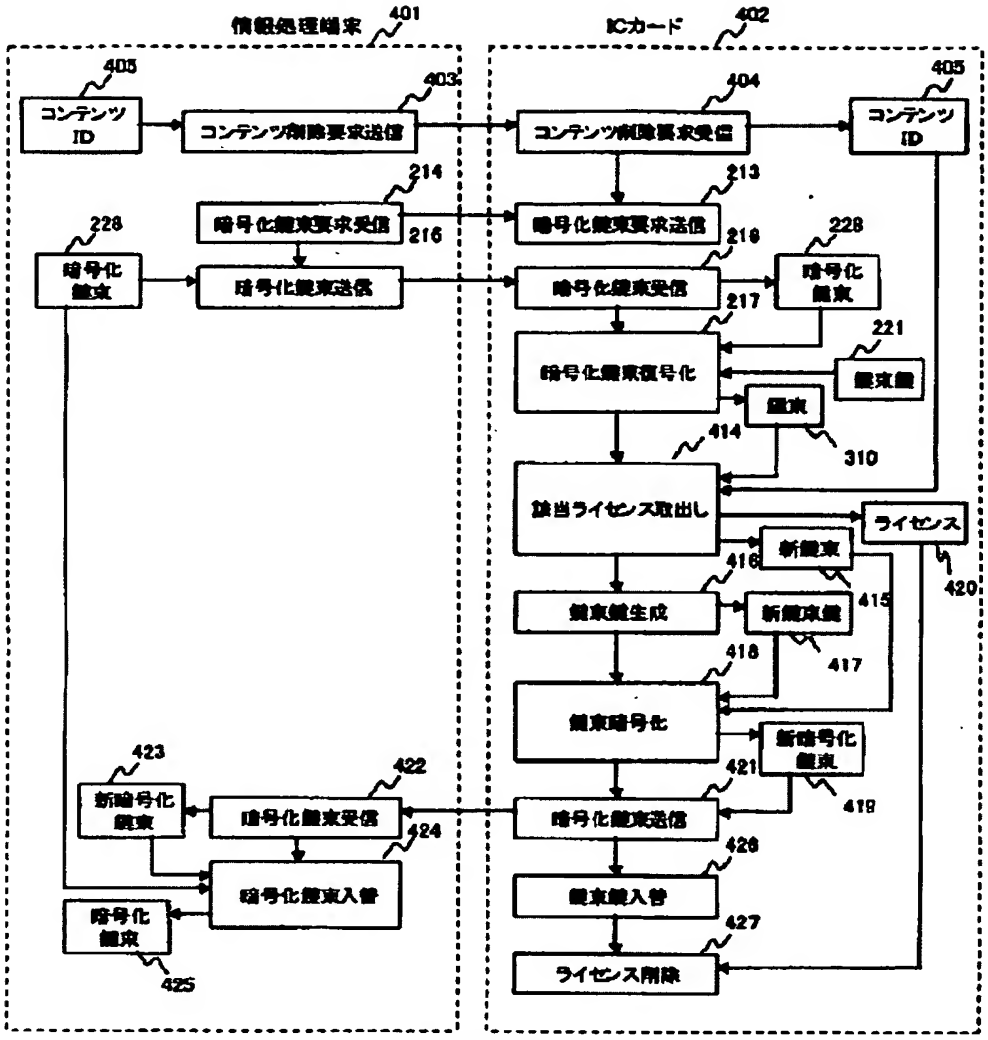


Figure 6

Key:
213 Encrypted key bundle request transmission
214 Encrypted key bundle request reception
215 Encrypted key bundle transmission
216 Encrypted key bundle reception
217 Encrypted key bundle decoding
221 Key-bundle key
228 Encrypted key bundle
310 Key bundle
401 Information processing terminal
402 IC card
403 Content deletion request transmission
404 Content deletion request reception

405 Content ID
414 Corresponding license fetching
415 New key bundle
416 Key-bundle key generation
417 New key-bundle key
418 Key bundle encryption
419 New encrypted key bundle
420 License
421 Encrypted key bundle transmission
422 Encrypted key bundle reception
423 New encrypted key bundle
424 Encrypted key bundle replacement
425 Encrypted key bundle
426 Key-bundle key replacement
427 License deletion

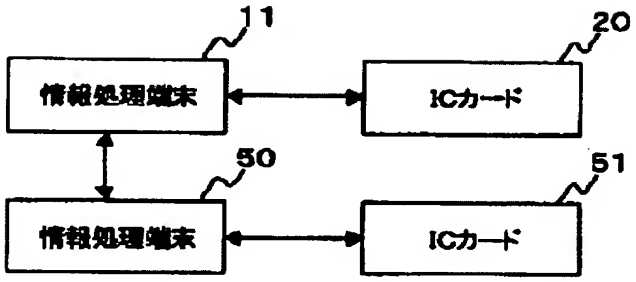


Figure 7

Key: 11 Information processing terminal
20 IC card
50 Information processing terminal
51 IC card

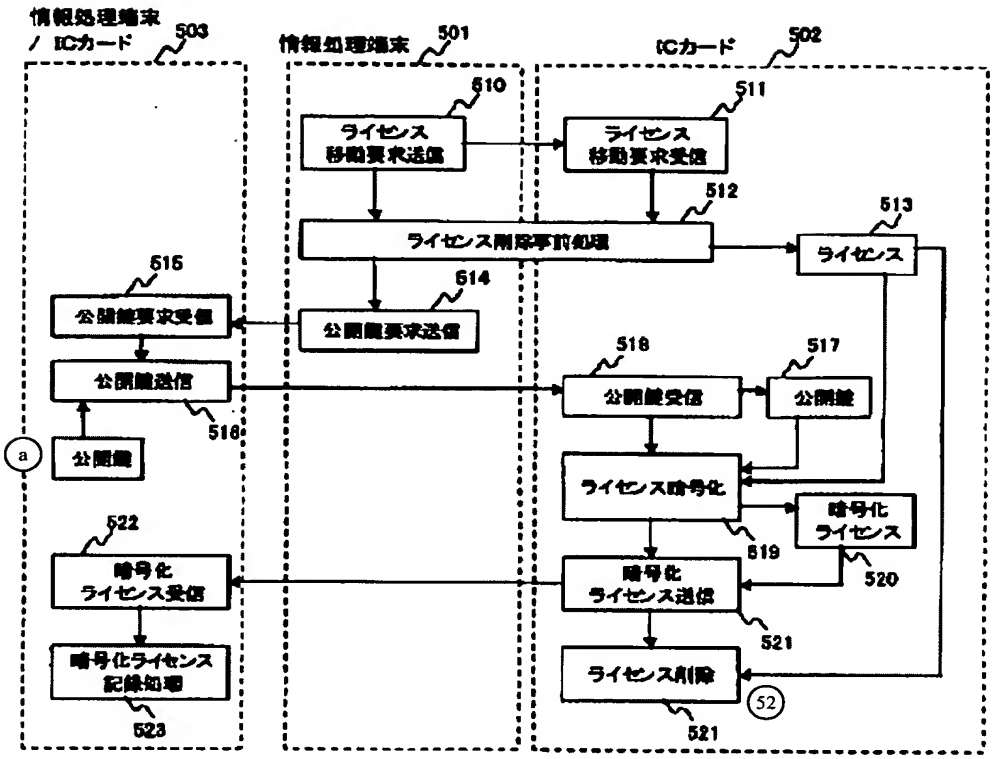


Figure 8

Key:

a	Public key
52	License deletion [labeled 521 in figure, 52 in text]
501	Information processing terminal
502	IC card
503	Information processing terminal/IC card
510	License movement request transmission
511	License movement request reception
512	Processing before license deletion
513	License
514	Public key request transmission
515	Public key request reception
516	Public key transmission
517	Public key
518	Public key reception
519	License encryption
520	Encrypted license
521	Encrypted license transmission
522	Encrypted license reception
523	Encrypted license recording processing